MODULE HANDBOOK

Bachelor of Science

Cyber Security (CSE-BACSE)

180 CP

Campus Studies

As of February 25th, 2025

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

Classification: Undergraduate

Contents

---

3. Semester

---

4. Semester

---

5. Semester

1. Semester

Operating Systems, Computer Networks, and Distributed Systems

Module Code: CSEBIBRVS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (Operating Systems, Computer Networks, and Distributed Systems)

Contributing Courses to Module

- Operating Systems, Computer Networks, and Distributed Systems (CSEBIBRVS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Operating systems
- Computer networks
- Distributed systems
- Mobile computing

Learning Outcomes

Operating Systems, Computer Networks, and Distributed Systems

On successful completion, students will be able to

- explain the basic functions of operating systems.
- compare different operating systems.
- explain and compare the OSI reference model and the TCP/IP protocol stack.
- explain the most important IP-based protocols and services and their application.
- explain and compare different architectures for distributed systems.
- explain and compare the main mobile communication networks.
- explain basic challenges of the security on the Internet and their solutions.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Operating Systems, Computer Networks, and Distributed Systems

Course Code: CSEBIBRVS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Operating systems are a central component of computers and provide their basic functions. To an increasing extent, however, computers do not stand alone, but are integrated into networks within which data and functions of other computer systems can be accessed. This enables distributed systems in which data and functions are systematically assigned to different computers in order to perform jointly defined tasks. While in the past, the various computers were stationary, many mobile computers are now also in use, which leads to completely new application scenarios in both private and business contexts.

Course Outcomes

On successful completion, students will be able to

- explain the basic functions of operating systems.
- compare different operating systems.
- explain and compare the OSI reference model and the TCP/IP protocol stack.
- explain the most important IP-based protocols and services and their application.
- explain and compare different architectures for distributed systems.
- explain and compare the main mobile communication networks.
- explain basic challenges of the security on the Internet and their solutions.

Contents

1. Foundations of Operating Systems
   - 1.1 Basic Structure of Computer Systems
   - 1.2 File Systems
   - 1.3 Memory Management
   - 1.4 Processes and Threads
2. Common Operating Systems
   - 2.1 Basic Concepts: Windows
   - 2.2 Basic Concepts: Unix and Linux
   - 2.3 Basic Concepts: Apple Operating Systems
   - 2.4 Mobile Operating Systems

3. Computer Networks
   - 3.1 Principles of Data Transmission
   - 3.2 The OSI Reference Model
   - 3.3 Network Topologies

4. TCP/IP And Internet
   - 4.1 Historical background
   - 4.2 TCP/IP Protocol Stack
   - 4.3 Selected IP-Based Protocols and Services
   - 4.4 Online Security

5. Architectures of Distributed Systems
   - 5.1 Client-Server Systems and Distributed Applications
   - 5.2 Basic Concepts of Distributed Systems: Concurrency, Semaphores, Deadlock
   - 5.3 Communication in Distributed Systems
   - 5.4 Service Orientation: SOA, Web Services and Microservices
   - 5.5 Cloud Applications
   - 5.6 Transactions in Distributed Systems
   - 5.7 High-Performance Computing Cluster

6. Mobile Computing
   - 6.1 Basics, Techniques and Protocols for Mobile Computing
   - 6.2 Mobile Internet and its Applications
   - 6.3 Mobile Communication Networks
   - 6.4 Security And Data Protection in Mobile Systems

Literature

Compulsory Reading

Further Reading

- Tanenbaum, A. S., & Bos, H. (2015). Modern operating systems (4th ed.). Pearson.
- Tanenbaum A. S., & Wetherall, D. J. (2014) . Computer networks (5th ed.). Pearson.
- van Steen, M., & Tanenbaum , A. S. (2017). Distributed systems. (3rd ed.). Pearson. Available online.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Introduction to Data Protection and Cyber Security

Module Code: CSEBCSIDPITS

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ralf Kneuper (Introduction to Data Protection and Cyber Security)

Contributing Courses to Module

- Introduction to Data Protection and Cyber Security (CSEBCSIDPITS01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Fundamentals of IT Security
- Data Protection
- IT Security Management
- Network and Communication Security

Learning Outcomes

Introduction to Data Protection and Cyber Security

On successful completion, students will be able to

- explain the terms and concepts of IT security and know the typical procedures and techniques which exist in each area.
- cite the legal regulations on data protection and explain their implementation.
- discuss in-depth IT security management and suitable measures for implementation.
- use their overview knowledge of activities and strategies for IT security in software and system development.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Introduction to Data Protection and Cyber Security

Course Code: CSEBCSIDPITS01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, the students are familiarized with important concepts from the field of IT security. Basic terms are introduced and discussed, and typical application fields, areas of IT security application, and typical procedures and techniques are introduced and described.

Course Outcomes

On successful completion, students will be able to

- explain the terms and concepts of IT security and know the typical procedures and techniques which exist in each area.
- cite the legal regulations on data protection and explain their implementation.
- discuss in-depth IT security management and suitable measures for implementation.
- use their overview knowledge of activities and strategies for IT security in software and system development.

Contents

1. Fundamentals of Data Protection and Cyber Security
   - 1.1 Conceptual Bases, Protection Goals
   - 1.2 Attacks and Threats
   - 1.3 Security Strategy
   - 1.4 Legal Regulations
2. Data Protection
   - 2.1 Data Protection as a Personal Right
   - 2.2 Basic Principles of Data Protection
   - 2.3 EU General Data Protection Regulation
   - 2.4 Further International Regulations on Data Protection
   - 2.5 Cross-Border Data Flow
   - 2.6 Data Protection in Everyday Life
3. Basic Functions of Cyber Security and Their Implementation
   - 3.1 Identification and Authentication
   - 3.2 Rights Management

3.3 Rights Check
3.4 Preservation of Evidence

4. Cyber Security Management
   4.1 Basic Concepts and Standards in Cyber Security Management
   4.2 Series of Standards ISO 2700x

5. Cyber Security Management in Everyday Life
   5.1 Password Management
   5.2 Data Backup
   5.3 Email Security
   5.4 Protection Against Viruses and Other Malware
   5.5 Protection Against Social Engineering Attacks

6. Network and Communication Security
   6.1 Firewall Technology
   6.2 Network Separation
   6.3 Security in WLAN, Mobile Networks, Bluetooth, and NFC

7. Cyber Security in the Development of Software and Systems
   7.1 Protection of the Development Environment
   7.2 Secure Development
   7.3 Common Criteria

Literature

Compulsory Reading

Further Reading

- Arnold, R. (2017). Cybersecurity: A business solution. An executive perspective on managing cyber risk. Threat Sketch.
- European Parliament and Council of the European Union. (2016). EU General Data Protection Regulation (GDPR): Regulation 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. Chapters 1—3 .
- Mattord, H., & Whitman, M. (2017). Management of information security. Cengage.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Mathematics: Analysis

Module Code: CSEBDSMFC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Robert Graf (Mathematics: Analysis)

Contributing Courses to Module

- Mathematics: Analysis (CSEBDSMFC01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Sequences and Series
- Functions and Inverse Functions
- Differential Calculus
- Integral Calculus
- Differential Equations

Learning Outcomes

Mathematics: Analysis

On successful completion, students will be able to

- summarize the basic concepts of analysis.
- illustrate the terms "sequences" and "series".
- explain the concept of a function and determine the inverse function where possible.
- compute derivatives and integrals using the standard rules of differentiation and integration.
- explain the relationship between differentiation and integration.
- solve simple linear differential equations.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Methods	All Bachelor Programs in the Business field

Mathematics: Analysis

Course Code: CSEBDSMFC01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Analysis is one of the essential basic subjects of mathematics. Originally developed to be able to formulate and solve problems of classical mechanics mathematically, in its present rigorous form it has become indispensable in numerous applications in the natural sciences and technology. This module aims to introduce the basic tool of differential and integral calculus and to explain their mutual interrelations. In addition, the concept of differential equations is explained and corresponding solution methods are discussed for simple cases.

Course Outcomes

On successful completion, students will be able to

- summarize the basic concepts of analysis.
- illustrate the terms "sequences" and "series".
- explain the concept of a function and determine the inverse function where possible.
- compute derivatives and integrals using the standard rules of differentiation and integration.
- explain the relationship between differentiation and integration.
- solve simple linear differential equations.

Contents

1. Sequences and Series
   - 1.1 Sequences: Convergence and Monotony
   - 1.2 Definition and Convergence
   - 1.3 Specific Sequences and Series
2. Functions and Inverse Functions
   - 2.1 Functions and Their Properties
   - 2.2 Exponential and Logarithmic Functions
   - 2.3 Trigonometric Functions
3. Differential Calculus
   - 3.1 First Derivative and Power Rule
   - 3.2 Differentiation Rules and Higher Derivatives
   - 3.3 Taylor Series and Taylor Polynomial

3.4 Curve Sketching
3.5 Outlook: Partial Derivatives

4. Integral Calculus
   4.1 The Indefinite Integral and Integration Rules
   4.2 The Definite Integral and the Fundamental Theorem of Calculus
   4.3 Volume and Lateral Surface of Solids of Revolution and Arc Length

5. Differential Equations
   5.1 Introduction and Basic Terms
   5.2 Solution of First-Order Linear Homogeneous Differential Equations
   5.3 Solution of First-Order Linear Non-Homogeneous Differential Equations
   5.4 Outlook: Partial Differential Equations

Literature

Compulsory Reading

Further Reading

- HELM Project (n.d.). Helping Engineers Learn Mathematics: 50 Workbooks. Available Online.
- Magnus, R. (2020). Fundamental Mathematical Analysis. Springer International Publishing.
- Pal Srimanta, & Bhunia Subodh C. (2015). Engineering Mathematics. Oxford University Press.
- Sydsæter, K., Hammond, P., Strom, A., & Carvajal, A. (2016). Essential mathematics for economic analysis (Fifth edition). Pearson Education.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Review Book
☑ Slides	☑ Online Tests

Introduction to Academic Work

Module Code: CSEBCSIAW

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Brigitte Huber (Introduction to Academic Work)

Contributing Courses to Module

- Introduction to Academic Work (CSEBCSIAW01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Basic Workbook (passed / not passed)	

Weight of Module

see curriculum

Module Contents

- Scientific Theoretical Foundations and Research Paradigms
- Application of Good Scientific Practice
- Methodology
- Librarianship: Structure, Use, and Literature Management
- Forms of Scientific Work at IU

Learning Outcomes

Introduction to Academic Work

On successful completion, students will be able to

- understand and apply formal criteria of a scientific work.
- distinguish basic research methods and identify criteria of good scientific practice.
- describe central scientific theoretical basics and research paradigms and their effects on scientific research results.
- use literature databases, literature administration programs, and other library structures properly; avoid plagiarism; and apply citation styles correctly.
- apply the evidence criteria to scientific texts.
- define a research topic and derive a structure for scientific texts.
- compile a list of literature, illustrations, tables, and abbreviations for scientific texts.
- understand and distinguish between the different forms of scientific work at IU.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Methods	All Bachelor Programs in the Business field

Introduction to Academic Work

Course Code: CSEBCSIAW01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The application of good scientific practice is one of the basic academic qualifications that should be acquired while studying. This course deals with the distinction between everyday knowledge and science. This requires a deeper understanding of the theory of science, as well as the knowledge of basic research methods and instruments for writing scientific texts. The students therefore gain initial insight into academic research and are introduced to the basic knowledge that will help them in the future to produce scientific papers. In addition, the students receive an overview of the different IU examination forms and insight into their requirements and implementation.

Course Outcomes

On successful completion, students will be able to

- understand and apply formal criteria of a scientific work.
- distinguish basic research methods and identify criteria of good scientific practice.
- describe central scientific theoretical basics and research paradigms and their effects on scientific research results.
- use literature databases, literature administration programs, and other library structures properly; avoid plagiarism; and apply citation styles correctly.
- apply the evidence criteria to scientific texts.
- define a research topic and derive a structure for scientific texts.
- compile a list of literature, illustrations, tables, and abbreviations for scientific texts.
- understand and distinguish between the different forms of scientific work at IU.

Contents

1. Theory of Science
   - 1.1 Introduction to Science and Research
   - 1.2 Research Paradigms
   - 1.3 Fundamental Research Decisions
   - 1.4 Effects of Scientific Paradigms on Research Design
2. Application of Good Scientific Practice
   - 2.1 Research Ethics
   - 2.2 Evidence Teaching

- 2.3 Data Protection and Affidavit
- 2.4 Orthography and Shape
- 2.5 Identification and Delimitation of Topics
- 2.6 Research Questions and Structure

3. Research Methods
   - 3.1 Empirical Research
   - 3.2 Literature and Reviews
   - 3.3 Quantitative Data Collection
   - 3.4 Qualitative Data Collection
   - 3.5 Mix of Methods
   - 3.6 Critique of Methods and Self-Reflection

4. Librarianship: Structure, Use, and Literature Management
   - 4.1 Plagiarism Prevention
   - 4.2 Database Search
   - 4.3 Literature Administration
   - 4.4 Citation and Author Guidelines
   - 4.5 Bibliography

5. Scientific Work at the IU – Research Essay
6. Scientific Work at the IU - Project Report
7. Scientific Work at the IU - Case Study
8. Scientific Work at the IU - Bachelor Thesis
9. Scientific Work at the IU – Oral Assignment
10. Scientific Work at the IU – Oral Project Report
11. Scientific Work at the IU - Colloquium
12. Scientific Work at the IU - Portfolio
13. Scientific Work at the IU - Exam

Literature
Compulsory Reading
Further Reading ▪ Bell, J., & Waters, S. (2018). Doing your research project: A guide for first-time researchers (7th ed.). Open University Press McGraw-Hill Education. ▪ Deb, D., Dey, R., & Balas, V. E. (2019). Engineering research methodology: A practical insight for researchers. Springer. ▪ Saunders, M., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students (8th ed.). Pearson. ▪ Veal, A. J. (2018). Research Methods for Leisure and Tourism (5th ed.). Pearson.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Basic Workbook (passed / not passed)

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Online Tests
☑ Video	☑ Guideline
☑ Slides	

Introduction to Programming with Python

Module Code: CSEBDSIPWP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Cosmina Croitoru (Introduction to Programming with Python)

Contributing Courses to Module

- Introduction to Programming with Python (CSEBDSIPWP01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Python as a programming language for data science
- Variables and built-in datatypes
- Statements and functions
- Error and exception handling
- Important Python data science modules

Learning Outcomes

Introduction to Programming with Python

On successful completion, students will be able to

- use fundamental Python syntax.
- recollect common elementary data types.
- recognize foundational programming concepts and their realization in Python.
- understand error handling and logging.
- create working programs.
- list the most important libraries and packages for data science.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology field

Introduction to Programming with Python

Course Code: CSEBDSIPWP01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course provides students with a foundational understanding of the Python programming language. Following an introductory exposition to the importance of Python for data science-related programming tasks, students will be acquainted with fundamental programming concepts like variables, data types, and statements. Building on this basis, the important notion of a function is explained and errors, exception handling, and logging are explicated. The course concludes with an overview of the most widely-used library packages for data science.

Course Outcomes

On successful completion, students will be able to

- use fundamental Python syntax.
- recollect common elementary data types.
- recognize foundational programming concepts and their realization in Python.
- understand error handling and logging.
- create working programs.
- list the most important libraries and packages for data science.

Contents

1. Introduction
   - 1.1 Why Python?
   - 1.2 Obtaining and installing Python
   - 1.3 The Python interpreter , IPython, and Jupyter
2. Variables and Data Types
   - 2.1 Variables and value assignment
   - 2.2 Numbers
   - 2.3 Strings
   - 2.4 Collections
   - 2.5 Files
3. Statements
   - 3.1 Assignment, expressions, and print

3.2 Conditional statements
3.3 Loops
3.4 Iterators and comprehensions

4. Functions
   4.1 Function declaration
   4.2 Scope
   4.3 Arguments

5. Errors and Exceptions
   5.1 Errors
   5.2 Exception handling
   5.3 Logs

6. Modules and Packages
   6.1 Usage
   6.2 Namespaces
   6.3 Documentation
   6.4 Popular data science packages

Literature

Compulsory Reading

Further Reading

- Barry, P. (2016). Head first Python: A brain-friendly guide. O'Reilly Media, Inc.
- Kapil, S. (2019). Clean Python: Elegant coding in Python. Apress.
- Lubanovic, B. (2019). Introducing Python (2nd ed.). O'Reilly.
- Lutz, M. (2013). Learning Python (5th ed.). O'Reilly.
- Matthes, E. (2015). Python crash course: A hands-on, project-based introduction to programming. No Starch Press.
- Müller, A. C., & Guido, S. (2016). Introduction to machine learning with Python: A guide for data scientists. O'Reilly Media, Inc.
- Ramalho, L. (2015). Fluent Python: Clear, concise, and effective programming. O'Reilly.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Statistics: Probability and Descriptive Statistics

Module Code: CSEBDSSPDS-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Veronica Mas (Statistics: Probability and Descriptive Statistics)

Contributing Courses to Module

- Statistics: Probability and Descriptive Statistics (CSEBDSSPDS01-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Probability
- Random variables
- Joint distributions
- Expectation and variance
- Inequalities and limit theorems

Learning Outcomes

Statistics: Probability and Descriptive Statistics

On successful completion, students will be able to

- define probability, random variable, and probability distribution.
- understand the concept of Bayesian statistics.
- grasp the definition of joint and marginal distributions.
- calculate expectation values and higher moments.
- comprehend important inequality equations and limit theorems.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Methods	All Bachelor Programs in the Business field

Statistics: Probability and Descriptive Statistics

Course Code: CSEBDSSPDS01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Statistical description and analysis are the foundations for data-driven analysis and prediction methods. This course introduces the fundamentals, beginning with a formal definition of probabilities and introduction to the concepts underlying Bayesian statistics.Random variables and probability density distributions are then discussed, as well as the concept of joint and marginal distributions. The importance of various discrete and continuous distributions and their applications is stressed.Characterizing distributions is an important aspect of describing the behavior of probability distributions. Students are familiarized with expectation values, variance, and covariance. The concepts of algebraic and central moments and moment-generating functions complement the characterization of probability distributions.Finally, this course focuses on important inequalities and limit theorems such as the law of large numbers or the central limit theorem.

Course Outcomes

On successful completion, students will be able to

- define probability, random variable, and probability distribution.
- understand the concept of Bayesian statistics.
- grasp the definition of joint and marginal distributions.
- calculate expectation values and higher moments.
- comprehend important inequality equations and limit theorems.

Contents

1. Probability
   - 1.1 Definitions
   - 1.2 Independent events
   - 1.3 Conditional probability
   - 1.4 Bayesian statistics
2. Random Variables
   - 2.1 Random Variables
   - 2.2 Distribution functions and probability mass functions
   - 2.3 Important discrete probability distributions
   - 2.4 Important continous probability distributions

3. Joint Distributions
   - 3.1 Joint distributions
   - 3.2 Marginal distributions
   - 3.3 Independent random variables
   - 3.4 Conditional distributions

4. Expectation and Variance
   - 4.1 Expectation of a random variable, conditional expectations
   - 4.2 Variance and covariance
   - 4.3 Expectations and variances of important probability distributions
   - 4.4 Algebraic and central moments
   - 4.5 Moment-generating functions

5. Inequalities and Limit Theorems
   - 5.1 Probability inequalities
   - 5.2 Inequalities for expectations
   - 5.3 The law of large numbers
   - 5.4 Central limit theorem

Literature

Compulsory Reading

Further Reading

- Downey, A.B. (2014). Think stats (2nd ed.). O'Reilly.
- Rohatgi, V. K., & Saleh, A. K. E. (2015). An introduction to probability and statistics. John Wiley & Sons, Incorporated.
- Triola , M.F. (2013). Elementary statistics. Pearson Education.
- Wagaman, A.S & Dobrow, R.P. (2021). Probability: With applications and R. Wiley.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Review Book
☑ Slides	☑ Online Tests

2. Semester

Object-oriented Programming with Java

Module Code: CSEBCSOOPJ

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Sebastian Lempert (Object-oriented Programming with Java)

Contributing Courses to Module

- Object-oriented Programming with Java (CSEBCSOOPJ01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Introduction to the Java language
- Java language constructs
- Introduction to object-oriented system developement
- Inheritance
- Object-oriented concepts
- Exception handling
- Interfaces

Learning Outcomes

Object-oriented Programming with Java

On successful completion, students will be able to

- describe the basic concepts of object-oriented modeling and programming, distinguishing them from one another.
- describe the basic concepts and elements of the Java programming language and have some experience in their use.
- independently create Java programs to solve concrete problems.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology field

Object-oriented Programming with Java

Course Code: CSEBCSOOPJ01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Operational information systems are usually planned and programmed to be object-oriented. Therefore, this course teaches the basic skills of object-oriented programming. Theoretical concepts are presented and practiced directly with the programming language Java.

Course Outcomes

On successful completion, students will be able to

- describe the basic concepts of object-oriented modeling and programming, distinguishing them from one another.
- describe the basic concepts and elements of the Java programming language and have some experience in their use.
- independently create Java programs to solve concrete problems.

Contents

1. Introduction to Object-Oriented System Development
   - 1.1 Object Orientation as a Way of Looking at Complex Systems
   - 1.2 The Object as a Basic Concept of Object Orientation
   - 1.3 Phases in the Object-Oriented Development Process
   - 1.4 Basic Principle of Object-Oriented System Development
2. Introduction to Object-Oriented Modeling
   - 2.1 Structuring Problems With Classes
   - 2.2 Identifying Classes
   - 2.3 Attributes as Properties of Classes
   - 2.4 Methods as Functions of Classes
   - 2.5 Associations between Classes
   - 2.6 Unified Modeling Language (UML)
3. Programming Classes in Java
   - 3.1 Introduction to the Java Programming Language
   - 3.2 Basic Elements of a Class in Java
   - 3.3 Attributes in Java

Literature
Compulsory Reading
Further Reading ▪ Freeman, E., Robson, E., Bates, B., & Sierra, K. (2014). Head first design patterns (A brain friendly guide). O'Reilly Media. ▪ Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1995). Design patterns: Elements of re-usable object-oriented software. Addison-Wesley. ▪ Liang, Y. D. (2018). Introduction to Java programming and data structures. Pearson Education. ▪ Liguiori, L. & Liguori, P. (2008). Java pocket guide: Instant help for Java. O'Reilly Media. ▪ Oracle (2017). The Java tutorials. Available online. ▪ Samoylov, N. (2019). Learn Java 12 programming: A step-by-step guide to learning essential concepts in Java SE 10, 11, and 12. Packt Publishing. ▪ Weisfeld M. (2019). The object-oriented thought process (5th ed.). Addison-Wesley.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Mathematics: Linear Algebra

Module Code: CSEBDSMFLA

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Robert Graf (Mathematics: Linear Algebra)

Contributing Courses to Module

- Mathematics: Linear Algebra (CSEBDSMFLA01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Matrix Algebra
- Vector Spaces
- Linear and Affine Transformations
- Analytical Geometry
- Matrix Decomposition

Learning Outcomes

Mathematics: Linear Algebra

On successful completion, students will be able to

- explain fundamental notions in the domain of linear equation systems.
- exemplify properties of vectors and vector spaces.
- summarize characteristics of linear and affine mappings.
- identify important relations in analytical geometry.
- utilize different methods for matrix decomposition.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Methods	All Bachelor Programs in the Business field

Mathematics: Linear Algebra

Course Code: CSEBDSMFLA01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Linear algebra is a fundamental subject in mathematics. Its historical origin lies in the development of solution techniques for systems of linear equations arising from geometric problems. Numerous scientific and engineering applications can be solved using its methods. This course introduces the foundations of linear algebra and its basic notions like vectors and matrices. It then builds upon this foundation by introducing the derivation of solution techniques for problems in analytical geometry.

Course Outcomes

On successful completion, students will be able to

- explain fundamental notions in the domain of linear equation systems.
- exemplify properties of vectors and vector spaces.
- summarize characteristics of linear and affine mappings.
- identify important relations in analytical geometry.
- utilize different methods for matrix decomposition.

Contents

1. Foundations
    - 1.1 Systems of Linear Equations
    - 1.2 Matrices: Basic Terms
    - 1.3 Matrix algebra
    - 1.4 Matrices as compact representations of linear equations
    - 1.5 Inverse and trace
2. Vector Spaces
    - 2.1 Definition
    - 2.2 Linear Combination and Linear Dependance
    - 2.3 Basis, Linear Envelope, and Rank
3. Linear and Affine Mapping
    - 3.1 Matrix Representation of Linear Mappings
    - 3.2 Image and Kernel

3.3 Affine Spaces and Subspaces
3.4 Affine Mapping

4. Analytical Geometry
   4.1 Norm
   4.2 Scalar Product
   4.3 Orthogonal Projections
   4.4 Outlook: Complex Numbers

5. Matrix Decomposition
   5.1 Determinant
   5.2 Eigenvalues and Eigenvectors
   5.3 Cholesky Decomposition
   5.4 Eigenvalue Decomposition and Diagonalisation
   5.5 Singular Value Decomposition

Literature

Compulsory Reading

Further Reading

- Aggarwal, C.C. (2020). Linear Algebra and Optimization for Machine Learning: A Textbook. Springer.
- Mathai, A. M., & Haubold, H. J. (2017). Linear algebra, a course for physicists and engineers (1st ed.) De Gruyter.
- Neri, F. (2019). Linear algebra for computational sciences and engineering (2nd ed.) Springer.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Review Book
☑ Slides	☑ Online Tests

Collaborative Work

Module Code: CSEBCSCW

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Karin Halbritter (Collaborative Work)

Contributing Courses to Module

- Collaborative Work (CSEBCSCW01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Oral Assignment	

Weight of Module

see curriculum

Module Contents

- Self-Directed and Collaborative Learning
- Networking and Cooperation
- Performance in (Virtual) Teams
- Communication, Arguments, and Being Convincing
- Potentials for Conflict and Managing Conflicts
- Self-Management and Personal Skills

Learning Outcomes

Collaborative Work

On successful completion, students will be able to

- design their own learning processes both self-directed and collaborative with analog and digital media.
- initiate face-to-face and virtual cooperation and select suitable methods for shaping collaboration even in an intercultural context and across disciplinary boundaries.
- assess different forms of communication in relation to the goals and requirements of different situations and to reflect on their own communication and argumentation behavior in order to be able to shape conducive collaboration also in an interdisciplinary context.
- recognize social diversity including cultural and professional differences as a value, and to name and apply tools to deal with them constructively.
- explain conflict potentials and the role of emotions in conflicts and to describe the use of systemic methods in the target- and solution-oriented handling of conflicts.
- analyze one's own resources, present methods of self-leadership and self-motivation, and derive appropriate strategies.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Business Administration & Management	All Bachelor Programmes in the Business field

Collaborative Work

Course Code: CSEBCSCW01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The course supports the students in building up and expanding important interdisciplinary competences for our networked world, and in doing so, students can take advantage of the opportunities for constructive cooperation with others. It presents essential forms and design possibilities of collaborative learning and working, imparts basic knowledge and tools for self-managed, flexible, and creative thinking, learning and acting and familiarizes students with the topics of empathy and emotional intelligence. Students are also encouraged to use the course contents. In this way, they promote their autonomous competence to act and their competence in the interactive application of tools and in interacting in heterogeneous groups.

Course Outcomes

On successful completion, students will be able to

- design their own learning processes both self-directed and collaborative with analog and digital media.
- initiate face-to-face and virtual cooperation and select suitable methods for shaping collaboration even in an intercultural context and across disciplinary boundaries.
- assess different forms of communication in relation to the goals and requirements of different situations and to reflect on their own communication and argumentation behavior in order to be able to shape conducive collaboration also in an interdisciplinary context.
- recognize social diversity including cultural and professional differences as a value, and to name and apply tools to deal with them constructively.
- explain conflict potentials and the role of emotions in conflicts and to describe the use of systemic methods in the target- and solution-oriented handling of conflicts.
- analyze one's own resources, present methods of self-leadership and self-motivation, and derive appropriate strategies.

Contents

1. Learning for a Networked World, in a Networked World
    - 1.1 Requirements and Opportunities in the “VUCA” World
    - 1.2 Learning, Knowing and Not-Knowing
    - 1.3 The 4C Model: Collective, Collaborative, Continuous, and Connected
    - 1.4 Monitoring Learning Behaviour

2. Networking & Cooperation
   - 2.1 Cooperation Partners
   - 2.2 Sustainable Relationships: Digital Interaction and Trust Building
   - 2.3 Organizing Collaboration
   - 2.4 Social Learning

3. Performance in (Online) Teams
   - 3.1 Goals, Roles, Organization and Performance Measurement
   - 3.2 Team Building and Team Flow
   - 3.3 Agile Project Management with Scrum
   - 3.4 Other Agile Methods

4. Communicating and Convincing
   - 4.1 Communication as Social Interaction
   - 4.2 Language, Images, Metaphors, and Stories
   - 4.3 Attitude: Open, Empathetic, and Appreciative Communication
   - 4.4 Active Listening
   - 4.5 Analyze Your Conversational and Argumentative Skills

5. Recognizing Conflict Potential — Managing Conflicts — Negotiating Effectively
   - 5.1 Respecting Diversity and Seizing Opportunities
   - 5.2 Empathy
   - 5.3 Systemic Solution Process Work
   - 5.4 Constructive Negotiation

6. Achieving Your Goals
   - 6.1 Effective Goal Setting
   - 6.2 The Agile Use of Time
   - 6.3 (Self-)Coaching Methods
   - 6.4 Self-Management and Motivation Strategies

7. Mobilizing Resources
   - 7.1 Recognizing Resources
   - 7.2 Reflection and Innovation
   - 7.3 Transfer Strength and Willpower

Literature
Compulsory Reading
Further Reading ▪ Baber, A., Waymon, L., Alphonso, A., & Wylde, J. (2015). Strategic connections: The new face of networking in a collaborative world. AMACOM. ▪ Kaats, E., & Opheij, W. (2014). Creating conditions for promising collaboration: Alliances, networks, chains, strategic partnerships. Springer. ▪ Martin, S. J., Goldstein, N. J., & Cialdini, R. B. (2014). The small BIG: Small changes that spark BIG influence. Profile Books. ▪ Oettingen, G. (2014). Rethinking positive thinking: Inside the new science of motivation. Current.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Online Tests
☑ Video	☑ Guideline
☑ Slides	

Introduction to Network Forensics

Module Code: CSEBCSEINF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	CSEBIBRVS01_E	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Stephan Spitz (Introduction to Network Forensics)

Contributing Courses to Module

- Introduction to Network Forensics (CSEBCSEINF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam	

Weight of Module

see curriculum

Module Contents

- Network protocols and services
- World Wide Web
- Log data analysis
- Network forensics

Learning Outcomes

Introduction to Network Forensics

On successful completion, students will be able to

- interact with the network at a low level.
- understand the idiosyncrasies of Internet protocols.
- understand how to read RFCs in self-study when protocols are modified, or new ones added.
- understand common attacks against these protocols.
- understand how encryption is used in the Internet, and how it can be subverted.
- deploy and use IDPS systems.
- recognize security events in a SIEM that uses the IDPS data.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Introduction to Network Forensics

Course Code: CSEBCSEINF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	CSEBIBRVS01_E

Course Description

Network forensics is the art and science of capturing, recording and analysis of network events in order to discover attacks. This requires an in-depth knowledge of the core Internet protocols, how they are used and how they can be attacked.In this course, we will look at the most commonly used network protocols in Internet-based networking. We take a practical approach and look at actual network traces to discover how protocols are layered on each other. At its core there is TCP/IP. Other protocols, like HTTP, are built on that layer. Others, like DNS are based on the alternative UDP protocol. The major services that make up the Internet will be discussed. For instance, DNS is a protocol, but also a distributed database system. The ICANN organization oversees IP addresses and they are allocated to regional organizations and distributed to Autonomous Systems. This requires routing which is handled by other protocols.Encryption is provided for confidentiality of data but often also for authentication and integrity reasons. It is implemented in a variety of forms with an equal variety of trade-offs.The forensic practitioner requires a variety of tools, ranging from simple probing tools to collection and analysis tools. These are usually packaged as Intrusion Detection and Prevention Systems as well as SIEMs for the actual analysis. However, security event data usually needs to be augmented with external data sources for accurate diagnosis, and a variety of data sources will be discussed.

Course Outcomes

On successful completion, students will be able to

- interact with the network at a low level.
- understand the idiosyncrasies of Internet protocols.
- understand how to read RFCs in self-study when protocols are modified, or new ones added.
- understand common attacks against these protocols.
- understand how encryption is used in the Internet, and how it can be subverted.
- deploy and use IDPS systems.
- recognize security events in a SIEM that uses the IDPS data.

Contents

1. Why network forensics?
    - 1.1 Goals of investigations
    - 1.2 Network evidence gathering
    - 1.3 Intrusion detection

- 1.4 (D)Dos detection and mitigation
- 1.5 Tools of the trade

2. Basic protocol layering
   - 2.1 Internet protocol hierarchy
   - 2.2 Connection and connectionless protocols
   - 2.3 Reading RFCs and related documentation

3. TCP vs UDP
   - 3.1 Connectionless UDP
   - 3.2 TCP Connection establishment
   - 3.3 Missing packets and retransmission
   - 3.4 SOCKS proxying
   - 3.5 Attacks against TCP and UDP

4. The Internet Protocol
   - 4.1 IP addresses, IPv4 and IPv6
   - 4.2 Obtaining an IPv4 and IPv6 addresses
   - 4.3 The role of ICANN
   - 4.4 IP Firewalls and IP Network Address Translation
   - 4.5 SOCKS Proxying Protocol and Attack Vector

5. Routing the link layer
   - 5.1 ARP (Address Resolution Protocol)
   - 5.2 RIP dynamic routing
   - 5.3 BGP peering
   - 5.4 Autonomous System numbers
   - 5.5 Attacks against routing

6. Domain Name System
   - 6.1 Host name hierarchy
   - 6.2 DNS as a distributed database
   - 6.3 DNSSEC
   - 6.4 SPF, DMARC and other special records

7. Common application layer protocols
   - 7.1 HTTP
   - 7.2 HTTP/2
   - 7.3 SMTP

8. Transport Layer Encryption
   - 8.1 SSH
   - 8.2 IPSEC
   - 8.3 TLS
   - 8.4 Man in the middle attacks
   - 8.5 Certificates and certificate authorities

9. Intrusion detection and prevention systems
   - 9.1 Sensor and event types
   - 9.2 Netflow monitoring
   - 9.3 Rules, false positive and false negatives
   - 9.4 SIEMs
   - 9.5 Attack prevention technologies

10. Correlation and enrichment data sources
    - 10.1 Enrichment of data
    - 10.2 DNS data sources: DNSBLs, passive DNS, DNS repositories
    - 10.3 AS numbers, IP blocks, GeoIP and WhoIs data
    - 10.4 Certificate Transparency
    - 10.5 Correlation methods

Literature

Compulsory Reading

Further Reading

- Cole, E., Krutz, R. L., & Conley, J. (2009). Network security bible. John Wiley & Sons.
- Kurose, J., & Ross, K. (2016). Computer networking: A top-down approach. Pearson Education.
- Stevens, F. (2014). TCP/IP illustrated (2nd ed., Vol. 1—The protocols). Pearson.Tanenbaum, A., & Wetherall, D. (2013). Computer networks. Pearson Education.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Practice Exam
- ☑ Online Tests

Requirements Engineering

Module Code: CSEBCSRE

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Andrew Adjah Sai (Requirements Engineering)

Contributing Courses to Module

- Requirements Engineering (CSEBCSRE01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Basics of requirements engineering
- Enterprise modeling
- Requirement determination techniques
- Techniques of requirements documentation
- Testing and coordination of requirements
- Managing requirements

Learning Outcomes

Requirements Engineering

On successful completion, students will be able to

- describe models of enterprise modeling relevant to IT support and have experience in modeling.
- understand techniques and methods for determining requirements of IT systems and be able to distinguish them from each other.
- understand techniques for the documentation of requirements on IT systems and have experience in their use.
- describe techniques for testing, coordinating, and managing the requirements of IT systems and be able to distinguish between them.
- independently select suitable techniques and methods of requirements engineering for given project situations.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Requirements Engineering

Course Code: CSEBCSRE01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The early phases of software development are largely characterized by the fact that functional and technical requirements for the IT system have to be determined. The determination of these requirements must be carried out extremely carefully because all of the following activities in the SW development process are planned and executed on the basis of documented requirements. In this course, procedures, methods, and models are covered, which make it possible to have a structured and methodical determination and documentation of requirements for operational information systems.

Course Outcomes

On successful completion, students will be able to

- describe models of enterprise modeling relevant to IT support and have experience in modeling.
- understand techniques and methods for determining requirements of IT systems and be able to distinguish them from each other.
- understand techniques for the documentation of requirements on IT systems and have experience in their use.
- describe techniques for testing, coordinating, and managing the requirements of IT systems and be able to distinguish between them.
- independently select suitable techniques and methods of requirements engineering for given project situations.

Contents

1. Fundamentals and Terms of Requirements Engineering
   - 1.1 Requirements Engineering in the Software Process
   - 1.2 Core Activities in Requirements Engineering
   - 1.3 What is a Requirement?
2. Determination of Requirements
   - 2.1 Determination of the System Context
   - 2.2 Determination of the Sources of Requirements
   - 2.3 Selection of the Appropriate Investigative Techniques
   - 2.4 Determine Requirements Using Techniques

3. Selected Investigative Techniques
   - 3.1 Creativity Techniques
   - 3.2 Interview Techniques
   - 3.3 Observation Techniques
   - 3.4 Prototyping

4. Documentation of Requirements
   - 4.1 Activities for Documenting Requirements
   - 4.2 Typical Elements of Requirements Documentation
   - 4.3 Forms of Documentation

5. Modeling of Processes
   - 5.1 Basics and Terms
   - 5.2 Modeling with the Business Process Model and Notation
   - 5.3 Modeling with Event Driven Process Chains

6. Modeling of Systems
   - 6.1 Fundamentals of Unified Modeling Language
   - 6.2 UML Use Case Diagram
   - 6.3 UML Activity Diagram
   - 6.4 UML Class Diagram
   - 6.5 UML State Diagram

7. Checking and Reconciling Requirements
   - 7.1 Activities for Checking and Reconciling Requirements
   - 7.2 Test Criteria
   - 7.3 Test Principles
   - 7.4 Testing Techniques
   - 7.5 Coordination of Requirements

8. Management of Prioritization Requirements and Techniques
   - 8.1 Managing Requirements
   - 8.2 Techniques for Prioritizing Requirements

Literature
Compulsory Reading
Further Reading ▪ Dick, J., Hull, E., & Jackson, K. (2017). Requirements engineering (4th ed.). Springer. ▪ Glinz, M., van Loenhoud, H., Staal, S., & Bühne, S. (2020). Handbook for the CPRE foundation level according to the IREB standard: Education and training for certified professional for requirements engineering (CPRE): Foundation level (Version 1.0.0). InternationalRequirements Engineering Board. ▪ Pohl, K., & Rupp, C. (2015). Requirements engineering fundamentals: A study guide for the certified professional for requirements engineering exam: Foundation level—IREB compliant (2nd ed.). Rocky Nook.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

System Pentesting Basics

Module Code: CSEBCSESPB_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (System Pentesting Basics)

Contributing Courses to Module

- System Pentesting Basics (CSEBCSESPB01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam	

Weight of Module

see curriculum

Module Contents

- Penetration testing process
- Host-based penetration testing
- Exploitation of network services
- Web App penetration testing
- System hardening
- Ethical hacking

Learning Outcomes

System Pentesting Basics

On successful completion, students will be able to

- understand the basic organizational and compliance needs for penetration testing.
- identify the relevant components of modern-day IT system that may be exploitable.
- understand the underlying processes comprising a penetration testing.
- understand the most common attack vectors associated to hosts, networks and Web Apps as well as how to defend against those.
- familiarize themselves with real-world tools used by professional penetration testers.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

System Pentesting Basics

Course Code: CSEBCSESPB01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

System penetration testing is a vital process for finding and supporting the mitigation of vulnerabilities in IT systems before the attackers can exploit them. For that reason, many organizations employ such "pentesters", or ethical hackers, to test their software and hardware base (connectivity included) and fix the security issues that are found. This has become a cornerstone of modern security concepts. However, in order to be successful in this endeavor, a good knowledge of the different types of targeted IT systems is required. We refer to hosts, networks, Web Apps, and even cloud computing. In this course we present the fundamental aspects of IT systems, along with the processes, tools and techniques that comprise the industrial practice of penetration testing. Equipped with this knowledge, students will understand the mechanisms of a given attack, and start down the path of pentesting themselves.

Course Outcomes

On successful completion, students will be able to

- understand the basic organizational and compliance needs for penetration testing.
- identify the relevant components of modern-day IT system that may be exploitable.
- understand the underlying processes comprising a penetration testing.
- understand the most common attack vectors associated to hosts, networks and Web Apps as well as how to defend against those.
- familiarize themselves with real-world tools used by professional penetration testers.

Contents

1. Penetration Testing Goals and Industrial Perspective
    - 1.1 Organizational Benefits
    - 1.2 Ethical Hacking Framework
    - 1.3 Legal and Compliance Aspects
    - 1.4 Responsible Disclosure of Vulnerabilities
    - 1.5 Professional Penetration Testing Services and Certifications
2. Background Concepts
    - 2.1 Operating Systems
    - 2.2 Hardware Architectures
    - 2.3 Networking and Protocols

- 2.4 Web-Based Applications
- 2.5 Cloud Computing

3. Penetration Testing Process
   - 3.1 Planning and Reconnaissance
   - 3.2 Whitebox, Blackbox and Graybox Scanning
   - 3.3 Gaining Access
   - 3.4 Maintaining Access
   - 3.5 Analysis and Reporting
   - 3.6 Hardening and Mitigation

4. Operating System-Based Penetration Testing
   - 4.1 Common Misconfigurations
   - 4.2 Shellcode Attacks
   - 4.3 Memory Corruption and Buffer Overflow Vulnerabilities
   - 4.4 Metasploit and Kali Tools
   - 4.5 Operating System Hardening

5. Network Penetration Testing
   - 5.1 Network Infrastructure Scoping and Recon
   - 5.2 Exploiting Network Services
   - 5.3 Lateral Movement in the Network
   - 5.4 Kerberos Attacks
   - 5.5 Toolset: Nmap, PowerShell, Bloodhound, and Tcpdump
   - 5.6 Devising Corrective Actions

6. Web App Penetration Testing
   - 6.1 The OWASP Methodology
   - 6.2 Open Source Intelligence (OSINT)
   - 6.3 Commonly Exploited Web App Vulnerabilities
   - 6.4 Exploitation Toolset: BurpSuite, sqlmap, BeEF and ExploitDB
   - 6.5 Reporting Findings and Mitigation Actions

7. Specialized Penetration Testing at a Glance
   - 7.1 Exploit Development
   - 7.2 Ethical Hacking
   - 7.3 Wireless and Mobile Device Penetration Testing
   - 7.4 Cloud Threat and Vulnerability Assessment

Literature
Compulsory Reading
Further Reading ▪ Hooley, G., Piercy, N., & Nicoulaud, B. (2011). Marketing strategy and competitive positioning (5th ed.). Prentice Hall. ▪ Kaplan, R., Norton, D., & Rugelsjoen, B. (2010). Managing alliances with the balanced scorecard. Harvard Business Review, 88(1/2), 114–120. ▪ Hackman, J. R., & Walton, R. E. (1986). Leading groups in organizations. In P. S. Goodman (Ed.), Designing effective work groups (pp. 72–119). Jossey-Bass.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

3. Semester

Intercultural and Ethical Decision-Making

Module Code: CSEBCSIDM

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Zeljko Sevic (Intercultural and Ethical Decision-Making)

Contributing Courses to Module

- Intercultural and Ethical Decision-Making (CSEBCSIDM01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Basics of Intercultural Competence
- Cultural Concepts
- Culture and Ethics
- Implications of Current Ethical Problems in the Area of Interculturality, Ethics, and Diversity
- Intercultural Learning and Working
- Case Studies for Cultural and Ethical Conflicts

Learning Outcomes

Intercultural and Ethical Decision-Making

On successful completion, students will be able to

- explain the most important terms in the areas of interculturality, diversity, and ethics.
- distinguish different explanatory patterns of culture.
- understand culture at different levels.
- plan processes of intercultural learning and working.
- understand the interdependencies of culture and ethics.
- independently work on a case study on intercultural competence.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Business Administration & Management	All Bachelor Programs in the Business field

Intercultural and Ethical Decision-Making

Course Code: CSEBCSIDM01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students acquire the necessary knowledge to understand intercultural competencies and current developments in the fields of diversity and ethics. Students will understand how to systematically plan and implement learning processes for the development of competences important in these areas. First, important terms are clarified and differentiated from each other, and cultural aspects are explained from different perspectives. In addition, students learn that cultural issues are relevant at different levels, for example, within a state, company, or other group. In this context, students also recognize the connection between ethics and culture with different interdependencies. On the basis of this knowledge, students are then familiarized with the different possibilities and potentials of intercultural and ethical learning and working. Practical cases are used to illustrate the importance of the relationships learned for today's work context in many companies. The students then work on a case study in which the acquired knowledge is systematically applied.

Course Outcomes

On successful completion, students will be able to

- explain the most important terms in the areas of interculturality, diversity, and ethics.
- distinguish different explanatory patterns of culture.
- understand culture at different levels.
- plan processes of intercultural learning and working.
- understand the interdependencies of culture and ethics.
- independently work on a case study on intercultural competence.

Contents

1. Basics of Intercultural and Ethical Competence to Act
    - 1.1 Subject Areas, Terms, and Definitions
    - 1.2 Relevance of Intercultural and Ethical Action
    - 1.3 Intercultural Action - Diversity, Globalization, Ethics
2. Cultural Concepts
    - 2.1 Hofstedes Cultural Dimensions
    - 2.2 Culture Differentiation According to Hall
    - 2.3 Locus of Control Concept to Rotter

3. Culture and Ethics
   - 3.1 Ethics - Basic Terms and Concepts
   - 3.2 Interdependence of Culture and Ethics
   - 3.3 Ethical Concepts in Different Regions of the World

4. Current Topics in the Area of Interculturality, Ethics, and Diversity
   - 4.1 Digital Ethics
   - 4.2 Equality and Equal Opportunities
   - 4.3 Social Diversity

5. Intercultural Learning and Working
   - 5.1 Acculturation
   - 5.2 Learning and Working in Intercultural Groups
   - 5.3 Strategies for Dealing with Cultural Conflicts

6. Case Studies for Cultural and Ethical Conflicts
   - 6.1 Case Study: Interculturality
   - 6.2 Case Study: Diversity
   - 6.3 Case Study: Interculturality and Ethics

Literature

Compulsory Reading

Further Reading

- Al-Ali, E., & Masmoudi, M. (2023). Leadership and Workplace Culture in the Digital Era. Business Science Reference.
- Barmeyer, C., Bausch, M., & Mayrhofer, U. (2021). Constructive Intercultural Management.
- Berrones-Flemmig, N., Contreras, F., & Dornberger, U. (2022). Business in the 21st century: A sustainable approach (1st ed.). Emerald Publishing Limited.
- Rossouw, J., & Van Vuuren, L. (2017). Business ethics (6th ed.). Oxford University Press Southern Africa.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Online Tests
☑ Video	☑ Guideline
☑ Slides	

Introduction to the Internet of Things

Module Code: CSEBINGEIT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Marian Benner-Wickner (Introduction to the Internet of Things)

Contributing Courses to Module

- Introduction to the Internet of Things (CSEBINGEIT01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Internet of Things Fundamentals
- Social and Economic Significance
- Communication Standards and Technologies
- Data Storage and Processing
- Design and Development
- Applicability

Learning Outcomes

Introduction to the Internet of Things

On successful completion, students will be able to

- grasp the distinctive features of Internet of Things (IoT) and IoT systems.
- understand the social and economic importance of Internet of Things.
- identify the most important standards for communication between IoT devices.
- differentiate between various techniques for storing and processing data in IoT systems.
- identify different architectures and technologies for structuring IoT systems.
- recognize challenges of data protection and data security in IoT systems.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software	All Bachelor Programmes in the IT & Technology field

Introduction to the Internet of Things

Course Code: CSEBINGEIT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of this course is to give students an insight into technical and theoretical basics of the Internet of Things (IoT) and its fields of application. In addition to the general structure of IoT systems and the technology standards used in them, students are also taught the importance of Internet of Things for economy and society. Furthermore, this course demonstrates how data is exchanged, stored and processed in IoT.

Course Outcomes

On successful completion, students will be able to

- grasp the distinctive features of Internet of Things (IoT) and IoT systems.
- understand the social and economic importance of Internet of Things.
- identify the most important standards for communication between IoT devices.
- differentiate between various techniques for storing and processing data in IoT systems.
- identify different architectures and technologies for structuring IoT systems.
- recognize challenges of data protection and data security in IoT systems.

Contents

1. Internet of Things Fundamentals
   - 1.1 The Internet of Things - Basics and Motivation
   - 1.2 Evolution of the Internet - Web 1.0 to Web 4.0
2. Social and Economic Significance
   - 2.1 Innovations for Consumers and Industry
   - 2.2 Implications on People and the World of Work
   - 2.3 Data Protection and Data Security
3. Communication Standards and Technologies
   - 3.1 Network Topologies
   - 3.2 Network Protocols
   - 3.3 Technologies
4. Data Storage and Processing

4.1 Networked Storage with Linked Data and RDF(S)
4.2 Analysis of Networked Data using a Semantic Reasoner
4.3 Processing of Data Streams with Complex Event Processing
4.4 Operation and Analysis of Large Data Clusters using NoSQL and MapReduce

5. Design and Development
5.1 Software Engineering for Distributed and Embedded Systems
5.2 Architectural Patterns and Styles for Distributed Systems
5.3 Platforms: Microcontrollers, Monoboard Computers, One-Chip Systems

6. Applicability
6.1 Smart Home / Smart Living
6.2 Ambient Assisted Living
6.3 Smart Energy / Smart Grid
6.4 Smart Factory
6.5 Smart Logistics

Literature

Compulsory Reading

Further Reading

- Buyya, R. & Vahid Dastjerdi, A. (Hrsg.) (2016). Internet of things. Principles and paradigms. Morgan Kaufmann, Cambridge (MA).
- Dian, F. J., & Vahidnia, R. (2020). IoT use cases and technologies. British Columbia Institute of Technology.
- Firouzi, F., Chakrabarty, K., & Nassif, S. (2020). Intelligent Internet of Things: From device to fog and cloud. Springer.
- Gilchrist, A. (2016). Industry 4.0. The industrial internet of things. Apress.
- Raj, P., & Raman, A. C. (2017). The Internet of things: enabling technologies, platforms, and use cases. CRC Press.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Algorithms, Data Structures, and Programming Languages

Module Code: CSEBCSL-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Musharaf Ahmed Doger (Algorithms, Data Structures, and Programming Languages)

Contributing Courses to Module

- Algorithms, Data Structures, and Programming Languages (CSEBCSL01-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Data Structures
- Algorithm Design
- Important Algorithms
- Programming Paradigms and the Basic Terms of Programming Languages
- Programme Analysis Tools
- Overview of Common Programming Languages

Learning Outcomes

Algorithms, Data Structures, and Programming Languages

On successful completion, students will be able to

- explain basic data structures and compare and apply them in concrete applications.
- explain basic algorithms.
- design, select and apply suitable algorithms and data structures for specific applications
- analyse sketched or programmed algorithms when or before running them
- explain and compare the common programming paradigms and programming languages.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology field

Algorithms, Data Structures, and Programming Languages

Course Code: CSEBCSL01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Programming essentially consists of selecting suitable algorithms and data structures for a specific task and converting them into program code. There are many different programming languages, which are based on different procedures and in which algorithms and data structures are implemented differently. In this module, these concepts, which have so far been dealt with using concrete examples, are systematically presented and applied more broadly in order to give students the necessary tools to develop a systematic approach to programming.

Course Outcomes

On successful completion, students will be able to

- explain basic data structures and compare and apply them in concrete applications.
- explain basic algorithms.
- design, select and apply suitable algorithms and data structures for specific applications
- analyse sketched or programmed algorithms when or before running them
- explain and compare the common programming paradigms and programming languages.

Contents

1. Basic Concepts
    - 1.1 Algorithms, Data Structures, and Programming Languages as the Basics of Programming
    - 1.2 Detailing and Abstraction
    - 1.3 Control Structures
    - 1.4 Types of Data
    - 1.5 Basic Data Structures (List, Chain, Tree)
2. Data Structures
    - 2.1 Advanced Data Structures: Queue, Heap, Stack, Graph
    - 2.2 Abstract Data Types, Objects, and Classes
    - 2.3 Polymorphism
3. Algorithm Design

- 3.1 Induction, Iteration, and Recursion
- 3.2 Methods of Algorithm Design
- 3.3 Correctness and Verification of Algorithms
- 3.4 Efficiency (Complexity) of Algorithms

4. Basic Algorithms
   - 4.1 Traversing and Linearization of Trees
   - 4.2 Search Algorithms
   - 4.3 Sorting Algorithms
   - 4.4 Search in Strings
   - 4.5 Hash Algorithms
   - 4.6 Pattern Recognition

5. Representing Structured Data
   - 5.1 Structure of XML Documents
   - 5.2 Accessing XML Documents Programmatically
   - 5.3 Transformation of XML Documents Using XSL
   - 5.4 JSON as an Alternative to XML

6. Measuring Programmes
   - 6.1 Type Inference and IDE Interactive Support
   - 6.2 Cyclomatic and Referential Complexity
   - 6.3 Digesting Code Documentation
   - 6.4 Compiler Optimization
   - 6.5 Code Coverage
   - 6.6 Unit and Integration Testing
   - 6.7 Heap Analysis

7. Programming Languages
   - 7.1 Programming Paradigms
   - 7.2 Execution of Programs
   - 7.3 Types of Programming Languages
   - 7.4 Syntax, Semantics, and Pragmatics
   - 7.5 Variables and Type Systems

8. Overview of Important Programming Languages
   - 8.1 Assembler and Webassembly
   - 8.2 C and C++

8.3 Java and C#
8.4 Haskell and Lisp
8.5 JavaScript and Its Relatives
8.6 Other Imperative Programming Languages

Literature

Compulsory Reading

Further Reading

- Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). Introduction to algorithms (4th ed.). MITPress.
- Sebesta, R. W. (2016). Concepts of programming languages (11th ed.). Pearson.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Online Tests
☑ Video	☑ Guideline
☑ Slides	

Theoretical Computer Science and Mathematical Logic

Module Code: CSEBCSTCSML

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Robert Graf (Theoretical Computer Science and Mathematical Logic)

Contributing Courses to Module

- Theoretical Computer Science and Mathematical Logic (CSEBCSTCSML01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Proposition and predicate logic
- Finite automata
- Formal languages
- Computability and Turing machines
- Complexity theory
- Petri nets

Learning Outcomes

Theoretical Computer Science and Mathematical Logic

On successful completion, students will be able to

- formulate and translate predicate logical relationships into programming languages.
- use finite automatons and regular expressions to describe technical facts.
- explain the Chomsky hierarchy.
- identify the limits of provability and predictability.
- explain the meaning and relevance of the P=NP problem.
- apply Petri nets for the description of technical facts.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Theoretical Computer Science and Mathematical Logic

Course Code: CSEBCSTCSML01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Theoretical computer science and mathematical logic form the theoretical basics of computer science. However, this is not "pure theory", as these fundamentals are applied in many areas of computer science. These include, for example, the formulation of conditions in SQL queries or other programs based on statement and predicate logic, the use of finite state machines to specify systems with state transition diagrams, and the modeling of business and other processes with Petri nets. In addition, theoretical computer science and mathematical logic analyze the limits of computer science and computability, which cannot be exceeded irrespective of the technologies and algorithms used.

Course Outcomes

On successful completion, students will be able to

- formulate and translate predicate logical relationships into programming languages.
- use finite automatons and regular expressions to describe technical facts.
- explain the Chomsky hierarchy.
- identify the limits of provability and predictability.
- explain the meaning and relevance of the P=NP problem.
- apply Petri nets for the description of technical facts.

Contents

1. Propositional Logic
   - 1.1 Basic Concepts
   - 1.2 Calculation Rules and Normal Forms
   - 1.3 Interpretation and Satisfiability
   - 1.4 Proof by Contradiction and Resolution
   - 1.5 Soundness and Completeness
2. Predicate Logic
   - 2.1 Basic Concepts
   - 2.2 Resolution in Predicate Logic
   - 2.3 Completeness and Incompleteness
   - 2.4 Logic Programming with Prolog

3. Finite Automata and Regular Expressions
   - 3.1 Basic Concepts of Finite Automata
   - 3.2 Regular Expressions and Languages
   - 3.3 Practical Applications

4. Formal Languages and Grammars
   - 4.1 Basic Concepts
   - 4.2 The Chomsky Hierarchy
   - 4.3 Context Free Languages (Type-2 Grammars)
   - 4.4 Context Sensitive Languages (Type-1 Grammars)

5. Computability and Turing Machines
   - 5.1 Models of Computability
   - 5.2 Turing Machines
   - 5.3 More Models of Computability
   - 5.4 Computability and Decidability and the Halting Problem

6. Complexity Theory
   - 6.1 Landau's Big O Notation
   - 6.2 Basic Concepts of Complexity Theory
   - 6.3 P=NP?
   - 6.4 NP-Complete Problems

7. Petri Nets
   - 7.1 Basic Concepts of Graphs and Petri Nets
   - 7.2 Modeling Properties of Concurrent Systems
   - 7.3 Reachability in Petri Nets
   - 7.4 Invariants in Petri Nets

8. Applications of Mathematical Logic and Theoretical Computer Science
   - 8.1 Parser and Compiler
   - 8.2 Program Verification
   - 8.3 Artificial Intelligence
   - 8.4 Cryptology

Literature
Compulsory Reading
Further Reading ▪ Sipser, M. (2014). Introduction to the theory of computation (3rd ed.). Cengage Learning. ▪ Huth, M., & Ryan, M. (2004). Logic in computer science: Modelling and reasoning about systems (2nd ed.). Cambridge University Press. ▪ Reisig, W. (2013). Understanding Petri nets: Modeling techniques, analysis methods, case studies. Springer. ▪ Parkes, A. P. (2008). A concise introduction to languages and machines. Springer. ▪ Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). Introduction to algorithms (4th ed.). MIT Press.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Review Book
☑ Slides	☑ Online Tests

IT Project Management

Module Code: CSEBCSEITPAM1

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Johannes Kent Walter (IT Project Management)

Contributing Courses to Module

- IT Project Management (CSEBCSEITPAM01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Basic terms and foundations of IT project management
- Large and small planning techniques
- Techniques for prioritization, cost-estimation, and project controlling
- Techniques for stakeholder, communication, and risk management
- Organization and structure in IT project management
- Schools of thought in IT project management

Learning Outcomes

IT Project Management

On successful completion, students will be able to

- explain and differentiate between the basic principles and tasks of IT project management.
- explain the important practical techniques and methods necessary for the implementation of IT project management.
- describe the basic procedural models and explain their advantages and disadvantages as well as their possible applications.
- identify possible project risks on the basis of given practical scenarios and select suitable measures from IT project management in order to minimize them in a targeted manner.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

IT Project Management

Course Code: CSEBCSEITPAM01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, typical problems in the management of Software projects are discussed and the methods and techniques used to address challenges conveyed.In addition, standard procedural models for IT project management are explained and their strengths and weaknesses specifically identified.

Course Outcomes

On successful completion, students will be able to

- explain and differentiate between the basic principles and tasks of IT project management.
- explain the important practical techniques and methods necessary for the implementation of IT project management.
- describe the basic procedural models and explain their advantages and disadvantages as well as their possible applications.
- identify possible project risks on the basis of given practical scenarios and select suitable measures from IT project management in order to minimize them in a targeted manner.

Contents

1. Basics Terms and Foundations of IT Project Management
   - 1.1 Definition of a Project and Types of IT Projects
   - 1.2 IT Project Lifecycle
   - 1.3 Multi-Project Management – The Project in the Context of the Organization
2. Planning Techniques
   - 2.1 Large-Scale Planning: Milestones, Sub-tasks, and Work Packages
   - 2.2 Large-Scale Planning: Gantt Charts
   - 2.3 Planning and Organization of Work Packages: Kanban Board
3. Prioritization, Estimation of Costs, Project Controlling
   - 3.1 Prioritization
   - 3.2 Estimation of Costs
   - 3.3 Project Controlling

4. Stakeholder, Communication and Risk Management
   - 4.1 Stakeholder Management
   - 4.2 Communication Management
   - 4.3 Risk Management

5. Organization and Structure in IT Project Management
   - 5.1 Overview and Levels of Management from PRINCE2
   - 5.2 Management Processes in PRINCE2
   - 5.3 Pragmatic IT Project Management (PITPM)
   - 5.4 Configuration of an IT Project in PITPM
   - 5.5 Management of a project in PITPM

6. Schools of Thought in IT Project Management
   - 6.1 Agile Software Development
   - 6.2 Value-Based Software Engineering

Literature

Compulsory Reading

Further Reading

- Project Management Institute. (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition and The Standard for Project Management (ENGLISH): Vol. Seventh edition. Project Management Institute.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

DevSecOps and Common Software Weaknesses

Module Code: CSEBCSEDCSW_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSESPB01_E or CSEBCSESPB01_E or DLBCSESPB01_D	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (DevSecOps and Common Software Weaknesses)

Contributing Courses to Module

- DevSecOps and Common Software Weaknesses (CSEBCSEDCSW01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Written Assignment	

Weight of Module

see curriculum

Module Contents

- Common code bugs
- Software Development Lifecycle
- DevOps
- DevSecOps
- Vulnerability reporting and bug bounty programs
- Patch management

Learning Outcomes

DevSecOps and Common Software Weaknesses

On successful completion, students will be able to

- avoid common software implementation and design mistakes.
- design a software development lifecycle process based on DevSecOps principles.
- incorporate vulnerability reporting and response into the SDL.
- organize and manage a bug bounty program.
- implement and manage a corporate patch management process.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

DevSecOps and Common Software Weaknesses

Course Code: CSEBCSEDCSW01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSESPB01_E or CSEBCSESPB01_E or DLBCSESPB01_D

Course Description

Modern organizations are run by software to some degree or another. In many cases, it is the custom software in business processes or products that is the key differentiator. But even companies that do no development of their own, are dependent on software and understanding software vulnerabilities is vital to their operations, as recent ransomware attacks have shown.In this course, we look at modern software development and lifecycle processes. Since its beginnings with Extreme Programming, there has been a shift away from the waterfall design to an agile development process. More recently, the Shift-Left movement has advocated for security to be considered from the start and not as an afterthought.In order to design secure software, it is naturally important to understand how insecurities creep into code. We look at the most important enumerations of software bugs: OWASP and Mitre's CWEs. Lastly, patch management has become the most import defensive tool for an organization. We look at this topic both from a software development perspective as well as from the customer's point of view.

Course Outcomes

On successful completion, students will be able to

- avoid common software implementation and design mistakes.
- design a software development lifecycle process based on DevSecOps principles.
- incorporate vulnerability reporting and response into the SDL.
- organize and manage a bug bounty program.
- implement and manage a corporate patch management process.

Contents

1. Introduction to the software development process
    - 1.1 Traditional software development: Waterfall design
    - 1.2 Iterative design
    - 1.3 Agile software development
    - 1.4 Operations as a separate process
    - 1.5 Infrastructure as code
    - 1.6 Merging Development and Operations: DevOps
2. DevOps best practices

- 2.1 Coding: code development and review, source code management tools, code merging.
- 2.2 Building: continuous integration tools, build status.
- 2.3 Testing: continuous testing tools that provide quick and timely feedback on business risks.
- 2.4 Packaging: artifact repository, application pre-deployment staging.
- 2.5 Releasing: change management, release approvals, release automation.
- 2.6 Configuring: infrastructure configuration and management, infrastructure as code tools.
- 2.7 Monitoring: applications performance monitoring, end-user experience.

3. Sources of security bugs
   - 3.1 General classes of bugs
   - 3.2 Looking at the OWASP top ten
   - 3.3 Looking at the Mitre CWE™

4. DevSecOps
   - 4.1 Protection goals
   - 4.2 Threat modeling
   - 4.3 Choice of programming language, tool chain and infrastructure
   - 4.4 Linting for code security issues
   - 4.5 Testing for security
   - 4.6 Security by design/Shifting Left
   - 4.7 Security as a people problem
   - 4.8 Designing in a bug reporting and response process
   - 4.9 Managing a bug bounty program

5. Patch management
   - 5.1 Dilemma: software update churn vs security
   - 5.2 Vulnerability disclosures and the Mitre CVE™ process
   - 5.3 Coordinated vulnerability disclosure
   - 5.4 Program security vs Software-as-a-Service patching
   - 5.5 Deployment strategies for catching bugs early

6. Summary and research problems

Literature
Compulsory Reading
Further Reading ▪ Forsgren, N., Humble, J., & Kim, G. (2018). Accelerate: The science behind DevOps: Building and scaling high performing technology organizations (Illustrated ed.). IT Revolution Press. ▪ Kim, G., Humble, J., Debois, P., Willis, J., & Forsgren, N. (2021). The DevOps handbook: How to create world-class agility, reliability, & security in technology organizations (2nd ed.). IT Revolution Press. ▪ Toesland, F. (2019). The rise of DevSecOps. Computer Weekly.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Online Tests
☑ Video	☑ Guideline
☑ Slides	

4. Semester

IT Service Management

Module Code: CSEBCSITSM-02

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. André Köhler (IT Service Management)

Contributing Courses to Module

- IT Service Management (CSEBCSITSM01-02)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- IT Service Management Basics and Terms
- ITIL 4 - Basics and Four Dimensions
- ITIL 4 - Service Value System
- ITIL 4 - Principles
- ITIL 4 - Practices
- Information Security Management

Learning Outcomes

IT Service Management

On successful completion, students will be able to

- identify the fundamentals and challenges of IT service management.
- describe the motivation and structure of the IT Infrastructure Library (ITIL), distinguish four dimensions, apply the service value system and identify concrete practices.
- describe and apply fundamentals of IT security management.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

IT Service Management

Course Code: CSEBCSITSM01-02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT service management is an approach to align and understand a company's IT as a service provider and supporter of operational and business processes. This course uses the IT Infrastructure Library (ITIL) to teach concepts, procedures and best practices in the area of IT service management (IT operations). In other words, it looks at the management of activities that take place after an IT system has been developed: IT operations as a continuous run of the productive day-to-day business of a company's IT departments.

Course Outcomes

On successful completion, students will be able to

- identify the fundamentals and challenges of IT service management.
- describe the motivation and structure of the IT Infrastructure Library (ITIL), distinguish four dimensions, apply the service value system and identify concrete practices.
- describe and apply fundamentals of IT security management.

Contents

1. IT Service Management Basics and Terms
   - 1.1 IT Services
   - 1.2 IT Service Management
   - 1.3 ITSM Frameworks
2. ITIL 4 - Basics and Four Dimensions
   - 2.1 Stakeholders, Services and Service Management
   - 2.2 Value Contribution of IT
3. ITIL 4 - Service Value System
   - 3.1 Basics and Overview
   - 3.2 Inputs, Outcome and Governance
   - 3.3 The Service Value Chain
   - 3.4 Continual Improvement
4. ITIL 4 - Principles

4.1 Overview
4.2 Value Orientation
4.3 Iterative Procedure and Feedback
4.4 Establish Collaboration and Visibility
4.5 Optimize and Automate

5. ITIL 4 - Practices
5.1 Overview
5.2 General Management Practices
5.3 Service Management Practices
5.4 Technical Practices

6. Information Security Management
6.1 Information Security Basics
6.2 Standards, Best Practices and Legal Requirements
6.3 Information Security Management with ISO/IEC 27001

Literature

Compulsory Reading

Further Reading

- Agutter, C. (2019). ITIL® foundation essentials ITIL 4 edition: The ultimate revision guide. ITGovernance Publishing.
- Axelos Limited. (2019). ITIL 4 foundation: ITIL 4 edition. The Stationery Office.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Cryptography

Module Code: CSEBCSCT-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ralf Kneuper (Cryptography)

Contributing Courses to Module

- Cryptography (CSEBCSCT01-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Protection Targets, Vulnerabilities, and Threats
- Foundations of Cryptology and its Core Components
- Basic Cryptographic Applications
- Authentication
- Single Computer Security
- Security Communication Network
- Security E-Commerce
- Secure Software Development

Learning Outcomes

Cryptography

On successful completion, students will be able to

- give an overview of different classes of cryptographic systems.
- give a basic description of symmetric cryptographic methods, in particular One-Time Pad, DES, and AES, and describe their operating principles by means of simple, concrete examples.
- describe the basic hash functions.
- describe basic asymmetric cryptographic methods, especially RSA, and their operating principles by means of simple, concrete examples.
- describe the areas of application of cryptographic procedures and their application scenarios.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Developement	All Bachelor Programs in the IT & Technology field

Cryptography

Course Code: CSEBCSCT01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course covers basic and targeted in-depth knowledge of cryptographic processes and the practical use of cryptographic systems. After an overview of cryptographic methods, hash functions, symmetric methods, and asymmetric methods are presented. The theoretical basics of selected procedures are taught and practically explained using simple examples. In addition, areas of application and application scenarios for cryptographic procedures are presented.

Course Outcomes

On successful completion, students will be able to

- give an overview of different classes of cryptographic systems.
- give a basic description of symmetric cryptographic methods, in particular One-Time Pad, DES, and AES, and describe their operating principles by means of simple, concrete examples.
- describe the basic hash functions.
- describe basic asymmetric cryptographic methods, especially RSA, and their operating principles by means of simple, concrete examples.
- describe the areas of application of cryptographic procedures and their application scenarios.

Contents

1. Protection Goals, Vulnerabilities, and Threats
   - 1.1 Protection Goals
   - 1.2 Vulnerabilities and Threats
2. Foundations of Cryptology and its Core Components
   - 2.1 Encoding
   - 2.2 Symmetrical Encryption
   - 2.3 Asymmetric Encryption
   - 2.4 One-way Functions and Cryptographic Hash Functions
3. Basic Cryptographic Applications
   - 3.1 Key Exchange and Hybrid Processes
   - 3.2 Digital Signature

- 3.3 Message Authentication Code
- 3.4 Steganographic Methods

4. Authentication
   - 4.1 Passwords and Public-Key-Certificates
   - 4.2 Challenge-Response-Procedure and Zero-Knowledge-Procedure
   - 4.3 Biometric Methods
   - 4.4 Authentication in Distributed Systems
   - 4.5 Identities Through Smartcards

5. Security of Single Computers
   - 5.1 Malware and Cookies
   - 5.2 Some Special Features of Operating Systems
   - 5.3 Web Server Security

6. Security in Communication Networks
   - 6.1 Security Problems and Defense Concepts
   - 6.2 Internet Standards for Communication Security
   - 6.3 Identity and Anonymity
   - 6.4 Security in Mobile and Wireless Communications

7. Security in E-Commerce
   - 7.1 Email Security
   - 7.2 Online Banking and Online Payments
   - 7.3 Electronic Money

8. Secure Software Development
   - 8.1 Threat Modeling
   - 8.2 Secure Software Design
   - 8.3 Techniques for Safe Programming

Literature
Compulsory Reading
Further Reading ▪ Paar, C. & Pelzl, J. (2010). Understanding Cryptography. A Textbook for Students and Practitioners. Springer. ▪ Singh, S. (1999). The code book [electronic resource] : the science of secrecy from ancient Egypt to quantum cryptography (1. ed.). Anchor Books. ▪ Smart, N. P. (2016). Cryptography Made Simple. Springer.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	25 h	0 h	155 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	☑ Guideline

IT Law

Module Code: CSEBCSIITL

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Brian Gannon (IT Law)

Contributing Courses to Module

- IT Law (CSEBCSIITL01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Basic Concepts of Legal Systems
- Internet and Domain Law
- Contracts
- Intellectual Property
- Data Protection / Privacy

Learning Outcomes

IT Law

On successful completion, students will be able to

- describe basic concepts of IT law.
- provide examples of different approaches to IT law in different countries.
- identify legal questions as they arise in IT.
- apply the core ideas of data protection and privacy in their work.
- distinguish the different types of contracts and intellectual property as they relate to IT.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Developement	All Bachelor Programs in the IT & Technology field

IT Law

Course Code: CSEBCSIITL01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The application of IT is embedded in a legal framework which computer scientists need to know and adhere to in their work. This applies to the way their own work is performed which, for example, may be governed by contracts with suppliers and/or customers. Computer scientists create and use intellectual property, and this leads to questions of copyright, software patents, etc. Beyond this, IT strongly influences the social environment and therefore needs to abide by regulations such as data protection. The goal of this module is to provide students with a basic understanding of these legal aspects so they can take them into account, apply them in simple cases, and recognize when more specialised legal knowledge is required. Since IT is a topic that connects different countries and legal frameworks, the course looks at some of the common legal questions as they are handled in the European Union, the USA, and India.

Course Outcomes

On successful completion, students will be able to

- describe basic concepts of IT law.
- provide examples of different approaches to IT law in different countries.
- identify legal questions as they arise in IT.
- apply the core ideas of data protection and privacy in their work.
- distinguish the different types of contracts and intellectual property as they relate to IT.

Contents

1. Basic Concepts of Legal Systems
   - 1.1 The Role of Law in IT
   - 1.2 Basic Concepts of the Legal System in the European Union
   - 1.3 Basic Concepts of the Legal System in the USA
   - 1.4 Basic Concepts of the Legal System in India
2. Internet and Domain Law
   - 2.1 Web Sites and the Law
   - 2.2 Net Neutrality
   - 2.3 Domain Registration
   - 2.4 Internet Crime

3. Contracts
   - 3.1 Types of IT Contracts
   - 3.2 Electronic Contracts and Electronic Signatures
   - 3.3 Licences
   - 3.4 Free and Open Source Software
   - 3.5 Buying and Selling Off-the-Shelf Software
   - 3.6 Software Development Contracts

4. Intellectual Property
   - 4.1 Brands, Trade Marks and Domain Names
   - 4.2 Copyright
   - 4.3 Software Patents
   - 4.4 Digital and Data Ownership

5. Data Protection/Privacy
   - 5.1 Basic Concepts of Data Protection
   - 5.2 Data Protection in the European Union: the GDPR
   - 5.3 Data Protection in the USA
   - 5.4 Data Protection in India
   - 5.5 Trans-Border Data Flows

Literature

Compulsory Reading

Further Reading

- Hoeren, T., & Pinelli, S. (2018). Agile programming – Introduction and current legal challenges. Computer Law & Security Review, 34(5), pp. 1131-1138. Retrieved from www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Hr.-Hoeren-29.10.pdf
- Lloyd, I. (2018). Information technology law (8th ed.). Oxford: Oxford University Press.
- Murray, A. (2019). Information technology law: The law and society (4th ed.). Oxford: Oxford University Press.
- Soma, J. T. (2014). Privacy law in a nutshell. St. Paul, MN: West Academic.
- Wikia.org. (n.d.). The IT law wiki [web encyclopedia]. Retrieved from https://itlaw.wikia.org/wiki/The_IT_Law_Wiki#

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Online Tests
☑ Video	☑ Guideline
☑ Slides	

Host and Software Forensics

Module Code: CSEBCSEHSF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSESPB01_E or CSEBCSESPB01_E or DLBCSESPB01_D	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (Host and Software Forensics)

Contributing Courses to Module

- Host and Software Forensics (CSEBCSEHSF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Tools and methods for host forensics
- Malware sandboxing and reverse engineering
- Report and presentation writing

Learning Outcomes

Host and Software Forensics

On successful completion, students will be able to

- understand the requirements on system forensics analysis.
- know the available tools and methods for evidence collection and analysis.
- understand the principles of Malware sandboxing and reversing.
- write reports and presentations with the target audience in mind.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Host and Software Forensics

Course Code: CSEBCSEHSF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSESPB01_E or CSEBCSESPB01_E or DLBCSESPB01_D

Course Description

Security officers will encounter security incidents on a regular basis nowadays and will be called upon to examine the damage. We look at both criminal and business policy violation investigations. In particular how to collect and evaluate evidence.We look at different types of unwanted activity and how these manifest themselves in the data we collect. With the appropriate tools, the evidence can be collected and if necessary, a Chain of Custody ensured using appropriate cryptographic methods.Capturing the files on the disk is standard practice in computer forensics. However, a part of the evidence collection process is also capturing information from the running system which includes memory and process capture.The collected evidence must be evaluated appropriately, and logical conclusions drawn from it. Often, possible Malware is found on the victim system. We look at two methods of analyzing the Malware: Sandboxing and Reverse engineering.The results are put in a report and consideration needs to be taken who the target audience of the report and possible presentation will be. Good communication is vital here.

Course Outcomes

On successful completion, students will be able to

- understand the requirements on system forensics analysis.
- know the available tools and methods for evidence collection and analysis.
- understand the principles of Malware sandboxing and reversing.
- write reports and presentations with the target audience in mind.

Contents

1. Principles of Computer Forensics
   - 1.1 Investigation Basics: Criminal vs. Business policy
   - 1.2 Policies, Legal Frameworks and Standards
   - 1.3 Expert Witnesses
2. Digital Evidence
   - 2.1 Types of Evidence
   - 2.2 Acquisition and Chain of Custody
   - 2.3 Identification

- 2.4 Evaluation
- 2.5 Presentation

3. Host Evidence Collection
   - 3.1 Software tools and Hardware Support
   - 3.2 Cryptographic Methods to ensure Integrity and Chain of Custody
   - 3.3 Steps for Crime Scene Search
   - 3.4 Cloud and Mobile Devices
   - 3.5 Hard drive and SSD

4. System Forensics
   - 4.1 Memory Analysis
   - 4.2 Process Dumps and Analysis
   - 4.3 Operation Systems Forensics
   - 4.4 Cloud Forensics

5. Sandboxing Malware
   - 5.1 Commercial and Open Source Tools
   - 5.2 Guest System Considerations
   - 5.3 Spoonfeeding unwilling, slow or delayed Malware
   - 5.4 Reading Sandbox Reports

6. Principles of Reverse Engineering
   - 6.1 Clean Room Environment
   - 6.2 Principles of Disassembly
   - 6.3 Machine Code
   - 6.4 Decompilation

7. Evaluation
   - 7.1 Connecting the Dots
   - 7.2 Finding the Root Cause
   - 7.3 Mapping to Mitre ATT&CK® Techniques, Tactics and Procedures
   - 7.4 Avoiding jumping to Conclusions

8. Presentation
   - 8.1 Report Writing
   - 8.2 Law Enforcement Collaboration
   - 8.3 Preparation for Court Presentation
   - 8.4 Preparation for Presentation to Management

Literature

Compulsory Reading

Further Reading

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing, Cham.
- Mitre ATT&CK®. https://attack.mitre.org/.
- Newman, R. C. (2007): Computer Forensics: Evidence Collection and Management. Auerbach Publications, Boca Raton, FL.
- Reddy, N. (2019): Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations. Apress, New York City, NY.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: https://beginners.re/ (last accessed: 24 August 2020).

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Artificial Intelligence

Module Code: CSEBDSEAIS1-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Kristina Schaaff (Artificial Intelligence)

Contributing Courses to Module

- Artificial Intelligence (CSEBDSEAIS01-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam	

Weight of Module

see curriculum

Module Contents

- History of AI
- Modern AI Systems
- Reinforcement Learning
- Natural Language Processing (NLP)
- Computer Vision

Learning Outcomes

Artificial Intelligence

On successful completion, students will be able to

- chart the historical developments in artificial intelligence.
- understand the approach of contemporary AI systems.
- comprehend the concepts behind reinforcement learning.
- analyze natural language using basic NLP techniques.
- scrutinize images and their contents.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology field

Artificial Intelligence

Course Code: CSEBDSEAIS01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The quest for artificial intelligence (AI) has captured humanity's interest for many decades and has been an active research area since the 1960s. This course will give a detailed overview of the historical developments, successes, and set-backs in AI, as well as modern approaches in the development of artificial intelligence such as generative AI. The course gives an introduction to reinforcement learning, a process similar to how humans and animals experience the world: exploring the environment and inferring the best course of action. The course also covers the principles of natural language processing and computer vision, both of which are key ingredients for an artificial intelligence to be able to interact with its environment.

Course Outcomes

On successful completion, students will be able to

- chart the historical developments in artificial intelligence.
- understand the approach of contemporary AI systems.
- comprehend the concepts behind reinforcement learning.
- analyze natural language using basic NLP techniques.
- scrutinize images and their contents.

Contents

1. History of AI
   - 1.1 Historical Developments
   - 1.2 AI Winter
   - 1.3 Expert Systems
   - 1.4 Notable Advances
2. Modern AI Systems
   - 2.1 Narrow versus General AI
   - 2.2 Application Areas
3. Reinforcement Learning
   - 3.1 What is Reinforcement Learning?
   - 3.2 Markov Chains and Value Function

3.3 Temporal-Difference and Q Learning

4. Natural Language Processing (NLP)
   - 4.1 Introduction to NLP and Application Areas
   - 4.2 Basic NLP Techniques
   - 4.3 Vectorizing Data
   - 4.4 Advanced NLP Models

5. Computer Vision
   - 5.1 Introduction to Computer Vision
   - 5.2 Image Representation and Geometry
   - 5.3 Feature Detection
   - 5.4 Semantic Segmentation
   - 5.5 Advanced Image Generation Techniques

Literature

Compulsory Reading

Further Reading

- Bear, M. F., Barry, W. S., & Paradiso, M. A. (2020). Neuroscience: Exploring the brain (4th ed.). Lippincott Williams & Wilkins.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
- Grus, J. (2019). Data science from scratch: First principles with Python. O'Reilly.
- Jurafsky, D., & Martin, J. H. (2022). Speech and language processing (3rd ed.). Prentice Hall.
- Morris, M. R., Sohl-Dickstein, J., Fiedel, N., Warkentin, T., Dafoe, A., Faust, A., Farabet, C., & Legg, S. (2024). Proceedings of the 41st International Conference on Machine Learning. PMLR, 235, 36308–36321.
- Russell, S. J., & Norvig, P. (2022). Artificial intelligence: A modern approach (4th ed., global ed.). Pearson.
- Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). Adaptive Computation and Machine Learning. MIT Press.
- Szeliski, R. (2022). Computer vision: Algorithms and applications (2nd ed.). Texts in Computer Science. Springer.
- Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30. Curran Associates, Inc.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Information Security Standards

Module Code: CSEBCSEISS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	None	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Andrew Adjah Sai (Information Security Standards)

Contributing Courses to Module

- Information Security Standards (CSEBCSEISS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Structure of the Information Security Standards
- Information Security Controls
- Information Security Management System (ISMS)
- Risk Management and Assessment

Learning Outcomes

Information Security Standards

On successful completion, students will be able to

- understand the general structure of information security standards.
- understand the normative content of the frameworks and standards.
- remember the required security controls.
- analyze existing Information Security Management Systems.
- evaluate Information Security Management Systems.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Information Security Standards

Course Code: CSEBCSEISS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	None

Course Description

Information security includes digital as well as non-digital information. The subset IT-Security deals only with electronical processed, stored and transferred information. Thus, information security is about the security referring to digital and non-digital assets of an organization.

Course Outcomes

On successful completion, students will be able to

- understand the general structure of information security standards.
- understand the normative content of the frameworks and standards.
- remember the required security controls.
- analyze existing Information Security Management Systems.
- evaluate Information Security Management Systems.

Contents

1. Introduction to Information Security
   - 1.1 Basic Definitions, Security Concepts and Information Security Objectives
   - 1.2 Standards and Regulatory Frameworks
   - 1.3 Security Standards: ISO 27000 Family and BSI Standards
   - 1.4 Information Security Management System (ISMS)
2. Initiating an Information Security Management System
   - 2.1 Initial Setup for the ISMS
   - 2.2 Analysis of the Organization
   - 2.3 Analysis of the Existing ISMS and Determination of the Maturity
   - 2.4 Defining the ISMS Scope and Security Policies
3. Implementation of the Information Security Management System
   - 3.1 Risk Assessment
   - 3.2 Statement of Applicability (SoA)
   - 3.3 Definition of the Organizational Structure for Information Security
   - 3.4 Document Management and Communication Plan
   - 3.5 Definition of Controls and Procedures

4. Controlling of the Information Security Management System
   - 4.1 Monitoring, Measurement, Analysis and Evaluation
   - 4.2 Internal Auditing
   - 4.3 Management Review

5. Improving of the Information Security Management System
   - 5.1 Treatment of Challenges and Non-conformities
   - 5.2 Continual Improvement
   - 5.3 Corrective and Preventive Action Plans

6. Controls of the Information Security Management System
   - 6.1 General Structure of Controls
   - 6.2 Controls of the ISO 27001 – Annex A
   - 6.3 Management of Controls
   - 6.4 Evaluating the Effectiveness of Controls

Literature

Compulsory Reading

Further Reading

- Alexander, D., Finch, A., & Sutton, D. (2013). Information Security Management Principles (2nd ed.). BCS, The Chartered Institute for IT.
- Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System: Security management based on ISO 27001 guidelines. Apress.
- Awad, A.I., Yen, N., & Fairhurst, M. (2018). Information security: Foundations, technologies and applications. The Institution of Engineering and Technology.
- van Publishing, H. (2015). Foundations of information security based on ISO27001 and ISO27002 (2nd ed.). Van Haren Publishing.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Online Tests
☑ Video	☑ Guideline
☑ Slides	

5. Semester

Seminar: Current Topics in Computer Science

Module Code: CSEBCSSCTCS

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Carsten Skerra (Seminar: Current Topics in Computer Science)

Contributing Courses to Module

- Seminar: Current Topics in Computer Science (CSEBCSSCTCS01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Research Essay	

Weight of Module

see curriculum

Module Contents

- This seminar deals with current topics of computer science. Students make a dive deep into a specific topic within a sub-discipline of their choice.

Learning Outcomes

Seminar: Current Topics in Computer Science

On successful completion, students will be able to

- discuss in-depth and insightfully a given topic in the field of computer science.
- write about a certain computer science topic in terms of important characteristics, connections, and insights in the form of a research essay.
- execute the basics of scientific work and implement them in the context of a research essay.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Developement.	All Bachelor Programmes in the IT & Technology field

Seminar: Current Topics in Computer Science

Course Code: CSEBCSSCTCS01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This seminar is an opportunity for students to deepen the broad knowledge they will have gained over the previous four semesters of the study program. Students will choose a topic of specific individual interest that is connected to a sub-discipline of computer science. If a student, for example, is interested in the application of artificial intelligence in a specific context, elaborating context-specific use cases from a literature review can be the theme of the essay. Feedback provided by the tutor will help students strengthen any weaknesses they may have in scientific writing and academic work and prepare students for writing their bachelor thesis.

Course Outcomes

On successful completion, students will be able to

- discuss in-depth and insightfully a given topic in the field of computer science.
- write about a certain computer science topic in terms of important characteristics, connections, and insights in the form of a research essay.
- execute the basics of scientific work and implement them in the context of a research essay.

Contents

- Computer science is a broad subject area with many very different facets, depending on the specific sub-discipline. This seminar will address this diversity by taking up current trends in the context of individually-prepared texts. Each participant must create an essay for this purpose. Possible topics include Java and web development, data modeling and database systems, requirements engineering, and core computer science disciplines like operating systems, computer networks, distributed systems, algorithms, data structures, and programming languages.

Literature
Compulsory Reading
Further Reading ▪ Brookshear, G. / Bylow, D. (2014): Computer science: An overview. 12th edition, Pearson, Boston, MA. ▪ Gruhn,V. / Striemer, R. (Eds.) (2018): The essence of software engineering. Springer International Publishing, Cham. ▪ Springer. (n.d.) Lecture Notes in Computer Science. Springer, Heidelberg. ▪ Tardos, E. (Ed.). (n.d.) Journal of the ACM.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
114 h	36 h	0 h	0 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Slides	☑ Guideline

Advanced Data Analysis

Module Code: CSEBDSEDA1

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Thomas Zöller (Advanced Data Analysis)

Contributing Courses to Module

- Advanced Data Analysis (CSEBDSEDA01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Business performance analytics
- Text mining
- Web- and social media analytics
- Experimentation and testing

Learning Outcomes

Advanced Data Analysis

On successful completion, students will be able to

- identify important design considerations for business KPIs.
- explain various topics in business process analytics.
- utilize established techniques for web data analytics.
- understand analytical approaches to text mining and semantic analysis.
- disambiguate relevant questions in social media analytics.
- use the techniques and methods for experimentation and testing.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology field

Advanced Data Analysis

Course Code: CSEBDSEDA01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course introduces several advanced analytics subjects of practical relevance. The subject areas covered span from business performance measurement and analytics, text mining, and web- and social media analytics to current trends in experimental design and setup. Along this journey topics such as the design of key performance indicators (KPIs), business process analytics, word frequency and semantic analysis, data science on clickstreams, social media interactions, and multi-armed bandit testing are addressed.

Course Outcomes

On successful completion, students will be able to

- identify important design considerations for business KPIs.
- explain various topics in business process analytics.
- utilize established techniques for web data analytics.
- understand analytical approaches to text mining and semantic analysis.
- disambiguate relevant questions in social media analytics.
- use the techniques and methods for experimentation and testing.

Contents

1. Business Performance Analytics
   - 1.1 KPI design considerations
   - 1.2 Common business performance indicators
   - 1.3 Business process mining
2. Text Analytics
   - 2.1 Word and document frequency (TF-IDF)
   - 2.2 Semantic analysis
3. Web Analytics
   - 3.1 Web metrics
   - 3.2 Clickstream analytics
   - 3.3 Recommender systems
4. Social Network Mining

4.1 Introduction to social media analytics
4.2 Mining common social media platforms

5. Testing and Experimentation
5.1 Practical A/B testing
5.2 Multivariate tests
5.3 Multi-armed bandit testing

Literature

Compulsory Reading

Further Reading

- Kaushik, A. (2009). Web analytics 2.0: The art of online accountability & science of customercentricity. Wiley.
- Lane, H., Howard, C., & Hapke, H. (2019). Natural language processing in action: Understanding, analyzing, and generating text with Python. Manning.
- Parmenter, D. (2019). Key performance indicators: Developing, implementing, and using winning KPIs (4th ed.). Wiley.
- Russell, M. A., & Klassen, M. (2019). Mining the social web: Data mining Facebook, Twitter, Linkedin, Instagram, Github, and more (3rd ed.). O'Reilly.
- Siroker, D., & Koomen, P. (2013). A/B testing: The most powerful way to turn clicks into customers. Wiley.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Project: Data Analysis

Module Code: CSEBDSEDA2

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Frank Passing (Project: Data Analysis)

Contributing Courses to Module

- Project: Data Analysis (CSEBDSEDA02)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Portfolio	

Weight of Module

see curriculum

Module Contents

Transfer of methodological knowledge to the implementation of real-world analytics use cases from the above-mentioned problem domains.

Learning Outcomes

Project: Data Analysis

On successful completion, students will be able to

- formulate and implement a real-world analytical use case.
- analyze the suitability of different possible approaches with respect to the project task.
- transfer acquired specialized analytical knowledge to real-world use cases.
- derive relevant design choices from the given project setting.
- make apposite choices with respect to implementation alternatives.
- select appropriate resources

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology field

Project: Data Analysis

Course Code: CSEBDSEDA02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The focus of this course is the implementation of a real-world, advanced analytics use case in the form of a student project. Primary subject areas for this practical work include business performance analytics, text mining, web- and social analytics, and experimentation and testing.The goal is for students to demonstrate they can transfer the theoretical knowledge acquired in Advanced Data Analysis (DLBDSEDA01) to an implementation scenario that closely mimics project work in a professional data science setting.

Course Outcomes

On successful completion, students will be able to

- formulate and implement a real-world analytical use case.
- analyze the suitability of different possible approaches with respect to the project task.
- transfer acquired specialized analytical knowledge to real-world use cases.
- derive relevant design choices from the given project setting.
- make apposite choices with respect to implementation alternatives.
- select appropriate resources

Contents

- This course covers the practical implementation of the approaches and techniques in a project-oriented setting. Each participant must produce a project report detailing and documenting their work. Project tasks are chosen from a list or suggested by the students in accord with the tutor.

Literature

Compulsory Reading

Further Reading

- Hapke, H., Howard, C., & Lane, H. (2019). Natural language processing in action. Manning Publications.
- Klassen, M., & Russell, M. A. (2019). Mining the social web (3rd ed.). O'Reilly Media.
- Ojeda, T., Bilbro, R., & Bengfort, B. (2018). Applied text analysis with Python. O'Reilly Media.
- Parmenter, D. (2020). Key performance indicators: Developing, implementing, and using winning KPIs (3rd ed.). John Wiley & Sons.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Portfolio

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
114 h	36 h	0 h	0 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Slides	☑ Guideline

Cloud Computing

Module Code: CSEBDSCC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Tianxiang Lu (Cloud Computing)

Contributing Courses to Module

- Cloud Computing (CSEBDSCC01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Cloud computing fundamentals
- Relevant enabling technologies for cloud computing
- Introduction to serverless computing
- Established cloud platforms
- Cloud offerings for data science and analytics

Learning Outcomes

Cloud Computing

On successful completion, students will be able to

- understand the fundamentals of cloud computing and cloud service models.
- recognize enabling technologies that underlie current cloud offerings.
- cite the principles of serverless computing.
- analyze characteristics of established cloud offerings.
- describe cloud options for data science and machine learning

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology field

Cloud Computing

Course Code: CSEBDSCC01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Many of the recent advances in data science, particularly machine learning and artificial intelligence, rely on comprehensive data storage and computing power. Cloud computing is one way of providing that power in a scalable way, without considerable upfront investment in hardware and software resources. This course introduces the area of cloud computing together with its enabling technologies. Moreover, the most cutting-edge advances like serverless computing and storage are illustrated. Finally, a thorough overview on popular cloud offerings, especially in regard to analytics capabilities, is given.

Course Outcomes

On successful completion, students will be able to

- understand the fundamentals of cloud computing and cloud service models.
- recognize enabling technologies that underlie current cloud offerings.
- cite the principles of serverless computing.
- analyze characteristics of established cloud offerings.
- describe cloud options for data science and machine learning

Contents

1. Introduction to Cloud Computing
   - 1.1 Fundamentals of Cloud computing
   - 1.2 Cloud Service Models
   - 1.3 Benefits and Risks
2. Enabling Technology
   - 2.1 Virtualization and Containerization
   - 2.2 Storage Technology
   - 2.3 Networks and RESTful Services
3. Serverless Computing
   - 3.1 Introduction to Serverless Computing
   - 3.2 Benefits
   - 3.3 Limitations

4. Established Cloud Platforms
   - 4.1 General Overview
   - 4.2 Google Cloud Platform
   - 4.3 Amazon Web Services
   - 4.4 Microsoft Azure
   - 4.5 Platform Comparison

5. Data Science in the Cloud
   - 5.1 Provider-independent services and tools
   - 5.2 Google Data Science and Machine Learning Services
   - 5.3 Amazon Web Services Data Science and Machine Learning Services
   - 5.4 Microsoft Azure Data Science and Machine Learning Services

Literature

Compulsory Reading

Further Reading

- Goessling, S., & Jackson, K. L. (2018). Architecting cloud computing solutions. Packt Publishing.
- Mahmood, Z., Puttini, R., & Erl, T. (2013). Cloud computing: Concepts, technology & architecture. Prentice Hall.
- Sehgal, N. K., & Bhatt, P. C. P. (2023). Cloud computing with security and scalability: Concepts and practices.
- Zonooz, P., Farr, E., Arora, K., & Laszewski, T. (2018). Cloud native architectures. Packt Publishing.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

IT Security Consulting

Module Code: DLBCSEEISC_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Rachel John Robinson (Technical and Operational IT Security Concepts) / Jetzabel Maritza Serna-Olvera (Project: Configuration and Application of SIEM Systems)

Contributing Courses to Module

- Technical and Operational IT Security Concepts (DLBCSEEISC01_E)
- Project: Configuration and Application of SIEM Systems (DLBCSEEISC02_E)

Module Exam Type

Module Exam	Split Exam
	Technical and Operational IT Security Concepts • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Configuration and Application of SIEM Systems • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Technical and Operational IT Security Concepts

- Network analysis and evaluation
- Protection Profiles
- Intrusion Detection Systems
- Network Monitoring
- Security Information and Event Management (SIEM)
- IT-Security evaluation and assessment

Project: Configuration and Application of SIEM Systems

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) Tool into an Enterprise IT-Environment. Students will need to consider practical aspects such as different data sources, data fusion and big data analytics methods and processing, as well as constraints such as data availability and multiple data formats.

Learning Outcomes

Technical and Operational IT Security Concepts

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Project: Configuration and Application of SIEM Systems

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Technical and Operational IT Security Concepts

Course Code: DLBCSEEISC01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-Systems and Networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructure require higher security mechanism regarding confidentiality, integrity and availability. Based on specific “Protection Profiles” high sophisticated tools, mechanisms and procedures need to be designed, implemented, configurated and operated.With this course the student will be able to evaluate given IT-Infrastructure, support the security-design of new IT-Systems and Networks by developing specific Protection Profiles, evaluate which technical and operational security measures and application are required and how these are integrated, configured and operated.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Contents

1. Network Analysis and Evaluation
    - 1.1 Layer Specific Threats and Vulnerabilities
    - 1.2 DATA Flow, Interdependencies and Interrelationships
    - 1.3 Vulnerability Scanning and Detection
    - 1.4 Supporting Tools and Techniques
2. Protection Profiles
    - 2.1 Reference Architecture Technology and Networking
    - 2.2 Risk Assessment, Residual Risk and Risk Management
    - 2.3 Security Requirements and Safeguards
    - 2.4 Security Evaluation of IT-Security Products

2.5 Accreditation of IT-Systems and Networks

3. Intrusion Detection Systems
   - 3.1 Detection Strategy
   - 3.2 Data Sources, Sensors
   - 3.3 Analytics
   - 3.4 Indicators of Compromise

4. Network Monitoring
   - 4.1 Threat Protection Systems
   - 4.2 Wireless Sensor Networks Technology
   - 4.3 Threat Information Sharing

5. Security Information and Event Management (SIEM)
   - 5.1 Technical and Operational DATA Sources
   - 5.2 DATA Fusion
   - 5.3 Network Norm Behavior
   - 5.4 Big Data Analysis – Transferring Technical Data for Operational Information
   - 5.5 Security Situation Picture, Situational Awareness
   - 5.6 Incident Response Strategies and Automated Responses

6. IT-Security Evaluation and Assessment
   - 6.1 IT-Security Metrics
   - 6.2 IT-Security Assessment

Literature

Compulsory Reading

Further Reading

- Federal Office for Information Security (BSI) (2018): IT-Grundschutz Profiles - Structural Description - COMMUNITY DRAFT.
- Hayden, L. (2010): IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education.
- McNab, C. (2016): Network Security Assessment: Know Your Network. 3. Auflage, O'Reilly UK Ltd.
- Miller, D. R. et al. (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Configuration and Application of SIEM Systems

Course Code: DLBCSEEISC02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEEISC01_E or DLBCSEEISC01_D

Course Description

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) Tool into an Enterprise IT-Environment. Students will need to consider practical aspects such as different data sources, data fusion and big data analytics methods and processing, as well as constraints such as data availability and multiple data formats. Furthermore, students will face the challenge to transfer technical data into operational Information to initiate valid responses. By the end of this course, students will have obtained well-founded knowledge of the integration of SIEM into enterprise IT infrastructure, applications and services.

Course Outcomes

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Contents

- This course focuses on practical aspects of the implementation of a SIEM into an enterprise IT infrastructure environment. Students start with a chosen use case and SIEM and then evaluate requirements which need to be fulfilled so that the SIEM can be used as part of an enterprise IT system / network. Students need to evaluate requirements for sensors, network monitoring, intrusion detection, data fusion, big data analytics, and translating technical data into operational information.
- Based on the available information, valid responses – including automated responses - will be identified and processed.
- All relevant artifacts and considerations are documented by the students in a project report.

Literature
Compulsory Reading
Further Reading ▪ Al-Sakib, K. P. (2016): The State of the Art in Intrusion Prevention and Detection. Routledge, Abingdon. ▪ Miller, D. et al (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY. ▪ Mitchell, H. B. (2007): Multi-Sensor Data Fusion: An Introduction. Springer Verlag, Berlin.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Social Engineering

Module Code: DLBCSEESE_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Social Engineering and Insider Threats) / N.N. (Project: Social Engineering)

Contributing Courses to Module

- Social Engineering and Insider Threats (DLBCSEESE01_E)
- Project: Social Engineering (DLBCSEESE02_E)

Module Exam Type

Module Exam	Split Exam
	Social Engineering and Insider Threats • Study Format "myStudies": Written Assessment: Case Study • Study Format "Distance Learning": Written Assessment: Case Study Project: Social Engineering • Study Format "myStudies": Oral Project Report • Study Format "Distance Learning": Oral Project Report

Weight of Module

see curriculum

Module Contents

Social Engineering and Insider Threats

- Social Engineering Methods
- Legal Aspects of Social Engineering
- Insider Threat Detection
- Security Policies and Regulations
- National and International Cooperation and Information Exchange

Project: Social Engineering

This course focuses on practical aspects to prevent, detect and recover from socialengineering driven attacks as well as threat deriving from hostile insiders.

Learning Outcomes

Social Engineering and Insider Threats

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Project: Social Engineering

On successful completion, students will be able to

- recognize the importance of the “Human Factor” in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Social Engineering and Insider Threats

Course Code: DLBCSEESE01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-systems and networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructures are of high interest for attackers to gain information (Cyber Espionage) to manipulate or destroy information and data as well as interrupt basic functions and services by compromising these systems and enterprises. One attack vector is targeted to the users and operators to misuse these people as workforce to break security policies and regulations. Social Engineering or social manipulation is widely used by adversaries to gain the necessary information to compromise IT-Infrastructures and to achieve their specific goals. Using methods of social engineering is very close to the so called “Insider Threat”. People from inside the organization act for various reasons against the security policies and regulations of their own enterprise. Revenge, dissatisfaction or sometimes criminal intent are reasons for such behavior. A combination of social engineering and “hostile insiders” is a gold nugget for all adversaries. Therefore, technical and organizational measures have to be developed and implemented to avert such threats. With this course, students will be able to recognize methods of social engineering and identify insider threats. They will be able to develop and implement preventive security policies and regulations as well as responsive security measures to counter these threats.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Contents

1. Social Engineering Methods

- 1.1 Phishing, Spear Phishing and Dynamite Phishing
- 1.2 Quid pro quo, Baiting, Media Dropping
- 1.3 Scareware, CEO-Fraud
- 1.4 Pretexting, Tailgating

2. Legal Aspects of Social Engineering
   - 2.1 Compliance, Code of Conduct
   - 2.2 Identity Theft
   - 2.3 Data Privacy

3. Insider Threat Detection
   - 3.1 Data Mining Techniques
   - 3.2 Application of Machine Learning Methods
   - 3.3 Comprehensive Framework for Insider Threat Detection and Response
   - 3.4 Self-assessment Tools for Evaluation
   - 3.5 Organizational Countermeasures and Awareness

4. Security Policies and Regulations
   - 4.1 Organizational Framework, Compliance, Code of Conduct
   - 4.2 Training and Awareness
   - 4.3 Protection of sensitive Information
   - 4.4 Security Monitoring and Incident Response

5. National and International Cooperation and Information Exchange
   - 5.1 Cooperation with Internet Service Providers (ISP) and IT-Security stakeholders
   - 5.2 Exchange Platforms and Forums for Tactics Techniques and Procedures (TTP´s) and Best Practices
   - 5.3 Cooperation with National Security Authorities

Literature
Compulsory Reading
Further Reading ▪ Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited. ▪ Company: TrustedSec. (Internet DEMO Version to subscribe) ▪ Robert W. Gehl; Sean T Lawson (2022): Social Engineering : How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication. Online verfügbar unter https://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=2932693&site=eds-live. ▪ Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann. ▪ Kennedy, D.: The Social-Engineer Toolkit (SET)

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Project: Social Engineering

Course Code: DLBCSEESE02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEESE01_E or DLBCSEESE01_D

Course Description

This project course will give students hands-on experience in the challenging task to prevent and counter social engineering attacks and eliminate or as a minimum mitigate the insider threat to the Enterprise IT-Systems and Networks. Students will need to consider practical aspects of social and psychological challenges – the so called "Human Factor" - as well as the application of technical toolkits to detect attacks driven by social engineering methods or caused by hostile insiders. Through this course Students will develop a complete overview of organizational, technical and procedural measures by analyzing the threat vector landscape, identify vulnerabilities and security gaps in the enterprise and develop and implement practical security policies and regulations, including security awareness campaigns, to prevent and recover from incidents caused by social engineering and insider threats.

Course Outcomes

On successful completion, students will be able to

- recognize the importance of the "Human Factor" in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Contents

- This project course focuses on practical aspects to prevent, detect and recover from social engineering driven attacks as well as threat deriving from hostile insiders. Students start with a chosen use case to analyze a tangible and successful social engineering campaign, identify the main attack vectors and learn how different activities on multiple levels concur to reach the objective or the attacker. Students need to analyze the security framework of the attacked enterprise, identify the vulnerability gaps and shortfalls that allowed the social engineering attack to be successful. Taking into account the "Human Factor" the students

will then develop organizational and technical security policies to show how a specific attack could have been prevented and the damage been avoided or mitigated. All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature
Compulsory Reading
Further Reading ▪ Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane. ▪ Company: TrustedSec. (Internet DEMO Version to subscribe) ▪ Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford. ▪ Kennedy, D.: The Social-Engineer Toolkit (SET)

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Mohammad Reza Rostami (Static and Dynamic Malware Analysis) / N.N. (Seminar: Sandbox Interpretation)

Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02_E)

Module Exam Type

Module Exam	Split Exam
	Static and Dynamic Malware Analysis • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "myStudies": Written Assessment: Research Essay • Study Format "Duales myStudium": Written Assessment: Research Essay • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module
see curriculum

Module Contents

Static and Dynamic Malware Analysis

- Objectives in Malware analysis
- Analysis Lab setup
- Tools of the trade
- Malware Classification
- Sandboxes
- Reversing
- Digging deeper

Seminar: Sandbox Interpretation

This course is about the practical application of Malware analysis techniques to real sandbox log files.

Learning Outcomes

Static and Dynamic Malware Analysis

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Seminar: Sandbox Interpretation

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Malware is a top compromise vector in cyber attacks. Analyzing the attacking Malware gives the security analyst insights into the methodology and intension of the attacker. There are a number of ways that Malware can be analyzed and this course will introduce the most common ones.

Course Outcomes

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Contents

1. Objectives in Malware Analysis
   - 1.1 Understanding Malware: Components, Types, and Analysis
   - 1.2 Forensics
   - 1.3 Root Cause Analysis
   - 1.4 The MITRE Attack Framework
   - 1.5 Best Practices for Malware Prevention and Mitigation
2. Analysis Lab Setup
   - 2.1 Building a Secure Malware Analysis Lab
   - 2.2 Stealth
   - 2.3 Isolation
   - 2.4 Honeypots
3. Tools of the Trade
   - 3.1 Virtual Machines
   - 3.2 Debugger
   - 3.3 Anti Debugging Mechanism
   - 3.4 Disassembler

4. Malware Classification
   - 4.1 Malware Triage and Classification
   - 4.2 Structure of a Virus
   - 4.3 Antivirus
   - 4.4 VirusTotal
   - 4.5 Yara
   - 4.6 AI-assisted Malware Analysis

5. Sandboxes
   - 5.1 Different Sandbox Concepts and Their Purposes
   - 5.2 Levels of Interaction
   - 5.3 Instrumentation
   - 5.4 Online Sandboxing Services
   - 5.5 Sandbox Detection and Evasion

6. Reversing
   - 6.1 Understanding Malware Analysis and Its Impact
   - 6.2 Unpacking, Decrypting, and De-Obfuscation
   - 6.3 Debugging Techniques
   - 6.4 Control Flow Analysis
   - 6.5 Library and System Calls

7. Digging Deeper
   - 7.1 Threat Intelligence Integration
   - 7.2 Analysis of JavaScript Code
   - 7.3 Memory Forensics
   - 7.4 Understanding and Debugging Rootkits

Literature

Compulsory Reading

Further Reading

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing.
- Mitre ATT&CK®. https://attack.mitre.org/
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: https://beginners.re/ (last accessed: 24 August 2020)

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	**Course Type**
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E

Course Description

In this course, we explore the most important tool in Malware analysis, the Sandbox and extract from the Sandbox logs the potential attacks exhibited by the Malware.

Course Outcomes

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Contents

- This course is about the practical application of Malware analysis techniques to real sandbox log files and extract the indicators of compromise and Malware objectives into a report.

Literature

Compulsory Reading

Further Reading

- Gregg, M. (2008): Build Your Own Security Lab: A Field Guide for Network Testing. Wiley, Hoboken, NJ.
- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.

Study Format myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

DevSecOps

Module Code: DLBCSEEDSO_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Jörn Fahsel (Techniques and methods for agile software development) / N.N. (Project: Agile DevSecOps Software Engineering)

Contributing Courses to Module

- Techniques and methods for agile software development (IWNF01_E)
- Project: Agile DevSecOps Software Engineering (DLBCSEEDSO01_E)

Module Exam Type

Module Exam

Split Exam

Techniques and methods for agile software development

- Study Format "myStudies": Exam, 90 Minutes
- Study Format "Distance Learning": Exam, 90 Minutes

Project: Agile DevSecOps Software Engineering

- Study Format "Distance Learning": Written Assessment: Project Report
- Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Techniques and methods for agile software development

- Characteristics and Principles of Agility
- Agility in Small Teams with SCRUM
- Agile Project Management
- Agile Requirements and Software Architecture Management
- Agile Testing
- Agile Delivery and Deployment

Project: Agile DevSecOps Software Engineering

This module provides the fundamental security principles for leveraging DevOps in software engineering, also known as the DevSecOps paradigm. Given a security-relevant scenario, this module will illustrate good DevSecOps practices like definition of security baselines, threat modelling approaches, and security automation as part of the continuous integration/continuous development (CI/CD) pipeline.

Learning Outcomes

Techniques and methods for agile software development

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Project: Agile DevSecOps Software Engineering

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Techniques and methods for agile software development

Course Code: IWNF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The goal of the course is to give students a deeper insight into the topic of agile software development. First of all, the basic characteristics and principles of agility are presented and discussed. Afterwards, it is shown how small projects and teams can use agile software engineering and how agile principles can be transferred and applied to large projects. Afterwards, agile techniques are taught for selected core activities in software engineering, with a focus on testing, delivery and deployment.

Course Outcomes

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Contents

1. Characteristics and Principles of Agility
   - 1.1 Features and Challenges of Software Projects
   - 1.2 Classification of Uncertainty
   - 1.3 Comparison of Agile and Classic Software Development
   - 1.4 Principles of Agility
2. Agility in Small Teams with Scrum
   - 2.1 Basics of SCRUM
   - 2.2 Central Management Artifact: Product Backlog
   - 2.3 Other Management Artifacts abd Tools
3. Agile Project Management
   - 3.1 Planning Levels in Agile Project Management

3.2 Agile Portfolio Management
3.3 Organization of Several Teams in One Project
3.4 Product and Release Planning

4. Agile Requirements and Software Architecture Management
4.1 Requirements Engineering in Agile Projects
4.2 Architecture Management in Agile Projects

5. Agile Testing
5.1 Basic Principles and Requirements for the Quality Assurance Organization
5.2 Test Levels and Agility
5.3 Test Automation

6. Agile Delivery and Deployment
6.1 Continuous Delivery Pipeline
6.2 Continuous Build and Continuous Integration
6.3 Acceptance Tests, Load Tests and Continuous Deployment

Literature

Compulsory Reading

Further Reading

- Biffl, S. et al. (Hrsg.) (2005): Value-Based Software Engineering. Springer, Berlin/Heidelberg.
- Highsmith, J. (2009): Agile Project Management: Creating Innovative Products. Addison Wesley, Upper Saddle River, NJ.
- Layton, M. C. (2012): Agile project management for dummies. John Wiley & Sons, New York, NY.
- Rubin, K. S. (2012): Essential Scrum: A Practical Guide to the Most Popular Agile Process. Addison Wesley, Upper Saddle River, NJ.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Agile DevSecOps Software Engineering

Course Code: DLBCSEEDSO01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	IWNF01_E or DLBWIWTMAS01

Course Description

This course covers the basic security principles for leveraging the DevSecOps approach in software engineering scenarios. The content of this course will illustrate the adoption of DevSecOps to continuously and holistically improve the security of an organization, rather than just focusing on protecting the underlying software infrastructure (as in the case of traditional non-agile methodologies). By presenting DevSecOps principles like threat modelling, definition of security baselines, security automation/tools, and continuous compliance monitoring, this course will teach how security can be integrated while developing a software engineering product.

Course Outcomes

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Contents

- Despite the broad adoption of DevOps in the industry, the integration of security principles into this paradigm (i.e., DevSecOps) is still an open challenge for many practitioners. In this course the students will learn fundamental DevSecOps concepts like threat modelling, definition of security baselines, continuous compliance monitoring, and integration of security automation in DevOps.

Literature
Compulsory Reading
Further Reading ▪ Johnson, E. (2020): Secure DevOps. A Practical Introduction. (URL: https://www.sans.org/ondemand/course/secure-dev-ops-a-practical-introduction [Retrieved: 15.08.2020]). ▪ Hsu, T. (2018): Hands-On Security in DevOps. Packt Publishing, UK. ▪ Microsoft. (2020): Secure DevOps. Making security principles and practices an integral part of DevOps while maintaining improved efficiency and productivity. (URL: https://www.microsoft.com/en-us/securityengineering/devsecops [Retrieved: 15.08.2020]). ▪ Schneider, C. (2015): Security DevOps. Staying secure in agile projects. (URL: https://owaspappseceurope2015.sched.com/event/378l/security-devops-staying-secure-in-agile-projects [Retrieved: 15.08.2020]). ▪ Yasar, H. (2016): An Introduction to Secure DevOps. Including Security in the Software Lifecycle. (URL: https://insights.sei.cmu.edu/devops/2016/11/an-introduction-to-secure-devops-including-security-in-the-software-lifecycle.html [Retrieved: 15.08.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Security in Complex Networks

Module Code: DLBCSEESCN_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Claudia Heß (IT Architecture Management) / Prof. Dr. Holger Klus (Project: IT Security Architecture)

Contributing Courses to Module

- IT Architecture Management (DLBCSEITPAM02)
- Project: IT Security Architecture (DLBCSEESCN01_E)

Module Exam Type

Module Exam	Split Exam
	IT Architecture Management • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: IT Security Architecture • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

IT Architecture Management

- Basic terms and foundations of IT enterprise architectures management
- IT application portfolio management
- Architecture governance
- Modeling of IT enterprise architectures
- Frameworks using TOGAF as an example
- Reference models and sample catalogues

Project: IT Security Architecture

Using well-known methods and techniques from the field of IT architecture management, students will be able to develop a well-grounded overview of IT-infrastructure regarding IT-strategy and strategic management. Students will understand and take advantage of typical concepts, methods and models for all tasks in the framework of architecture management. Emphasis will be taken to the security aspects of the IT infrastructure by designing and implementing IT-security architecture in the overall framework.

Learning Outcomes

IT Architecture Management

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Project: IT Security Architecture

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

IT Architecture Management

Course Code: DLBCSEITPAM02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In addition to concrete IT projects, such as the development of a new IT system or the introduction of standard software, a strategic management system for organizational-wide IT infrastructure – that is, for all IT hardware and software systems – must be used.Strategic management is the responsibility of the IT enterprise architect, who operates IT architecture management. Their task is to strategically align IT infrastructure with an organization's business and IT strategy.This course covers the typical concepts, methods, procedures, and IT models of architecture management.

Course Outcomes

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Contents

1. Basic Terms and Foundation for the Management of IT Enterprise Architectures
   - 1.1 IT Enterprise Architecture
   - 1.2 Goals of Enterprise Architecture Management
   - 1.3 Processes in the Management of IT Enterprise Architectures
2. IT Application Portfolio Management
   - 2.1 IT Application Portfolio Management Overview
   - 2.2 Application Manual
   - 2.3 Portfolio Analysis
   - 2.4 Development Planning
3. Architecture Governance

3.1 Organizational Structure
3.2 Policy Development and Enforcement
3.3 Project Support

4. Modeling of IT Enterprise Architectures
   4.1 Models in the Context of IT Architecture Management
   4.2 Forms of Documentation for Processes and Applications
   4.3 Forms of Documentation for Systems and Technologies

5. Frameworks Using the Example of TOGAF
   5.1 Fundamentals and Use of IT Architecture Frameworks
   5.2 Overview and Categories of EAM Frameworks
   5.3 The Open Group Architecture Framework (TOGAF)

6. Reference Models and Sample Catalogues
   6.1 Architecture Reference Models
   6.2 EAM Design Sample Catalogue

Literature

Compulsory Reading

Further Reading

- Ahlemann, F., Messerschmidt, M., Stettiner, E., & Legner, C. (2012). Strategic enterprise architecture management. Challenges, best practices, and future developments. Springer-Verlag.
- Perroud, T., & Inversini, R. (2013). Enterprise architecture patterns: Practical solutions for recurring IT-architecture problems. Springer.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Slides	

Project: IT Security Architecture

Course Code: DLBCSEESCN01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEITPAM02 or IAMG01

Course Description

Using methods and techniques from the field IT architecture management, students will work independently on a practical question of IT security architecture. By the end of this course students will be able to independently develop IT security architecture models, based on an existing IT-system / network architecture.

Course Outcomes

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Contents

- Implementation and documentation of practical questions regarding IT security in the framework of IT architecture management. Typical scenarios are, for example, “Implementation of IT security devices in complex networks”, “Design of processes for security updates and patch management” and “using in-house resources or outsourcing of IT security tasks”.

Literature
Compulsory Reading
Further Reading ▪ Calder, Alan. (2020). Cyber Security - Essential Principles to Secure Your Organisation. IT Governance Publishing. ▪ Dr. Erdal Ozkaya (2019): Cybersecurity: The Beginner's Guide: A Comprehensive Guide to Getting Started in Cybersecurity. ▪ Pierre Bernard (2012): COBIT® 5 - A Management Guide. Online verfügbar unter https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1558038&site=eds-live. ▪ Virgilio Viegas; Oben Kuyucu (2022): IT Security Controls: A Guide to Corporate Standards and Frameworks.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Slides	☑ Guideline

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Mohammad Reza Rostami (Protocols, Log- and Dataflow-Analysis in Depth) / Dr. Jetzabel Maritza Serna-Olvera (Seminar: Threat Hunting, Analysis and Incident Response)

Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02_E)

Module Exam Type

Module Exam

Split Exam

Protocols, Log- and Dataflow-Analysis in Depth

- Study Format "Duales myStudium": Exam, 90 Minutes
- Study Format "myStudies": Exam, 90 Minutes
- Study Format "Distance Learning": Exam, 90 Minutes

Seminar: Threat Hunting, Analysis and Incident Response

- Study Format "Duales myStudium": Written Assessment: Research Essay
- Study Format "Distance Learning": Written Assessment: Research Essay
- Study Format "myStudies": Written Assessment: Research Essay

Weight of Module
see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Network Basics
- Operating System Logs
- Packet Capturing and Analysis
- Log Management
- Preparation for Attacks
- Intrusion Detection and Prevention System

Seminar: Threat Hunting, Analysis and Incident Response

- Mitre ATT&CK TTPs
- APT actors
- Security coverage gap analysis

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Seminar: Threat Hunting, Analysis and Incident Response

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Contents

1. Introduction to Network Forensics
    - 1.1 Basics of Network Forensics
    - 1.2 Evidence Handling Standards
    - 1.3 Verification of Evidence
2. Network Basics
    - 2.1 Protocol Basics and Functionality
    - 2.2 Difference between the OSI Model and TCP/IP Architecture
    - 2.3 Basics of TCP and UDP including Ports and Protocols
    - 2.4 DNS, DHCP and ARP
3. Host-Side Artifacts
    - 3.1 Network-based Artifacts stored in the Operating Systems
    - 3.2 Services and Ports
    - 3.3 TCP Connection States
    - 3.4 Tools for extracting the Artifacts

4. Packet Capture and Analysis
   - 4.1 Capturing Packets
   - 4.2 Tools like TCPDump and Wireshark
   - 4.3 Analysis of captured Packets

5. Location Information
   - 5.1 Impact of Time Zones on Investigations
   - 5.2 Location Information from the Network
   - 5.3 Location-based Services with Web Applications
   - 5.4 Location Information from WiFi

6. Preparing for Attacks
   - 6.1 Manage Netflow Data
   - 6.2 Loggings
   - 6.3 Antivirus
   - 6.4 SIEM and Incident Response

7. Intrusion Detection and Prevention Systems
   - 7.1 Detection Styles
   - 7.2 Host-based versus Network-based
   - 7.3 Challenges with Intrusion Detection and Prevention Systems
   - 7.4 Firewall and Application Logs

8. Correlation of Data
   - 8.1 Synchronization of Time across Multiple Systems
   - 8.2 Log Aggregation and Management
   - 8.3 Importance of Timelines

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- NIST Special Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studium Generale I and II

Module Code: DLBSG_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Studium Generale I) / N.N. (Studium Generale II)

Contributing Courses to Module

- Studium Generale I (DLBSG01_E)
- Studium Generale II (DLBSG02_E)

Module Exam Type

Module Exam	Split Exam
	Studium Generale I • Study Format "myStudies": See Selected Course • Study Format "Distance Learning": See Selected Course Studium Generale II • Study Format "Distance Learning": See Selected Course • Study Format "myStudies": See Selected Course

Weight of Module

see curriculum

Module Contents

Studium Generale I

In principle, all IU bachelor courses can be selected as courses for the "Studium Generale", so that the content can be chosen from the entire breadth of the IU distance learning program.

Studium Generale II

In principle, all IU bachelor courses can be selected as courses for the "Studium Generale", so that the content can be chosen from the entire breadth of the IU distance learning program.

Learning Outcomes

Studium Generale I

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Studium Generale II

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Links to other Modules within the Study Program	Links to other Study Programs of the University
It is a stand-alone offering with possible references to various required and elective modules	All IU Distance Learning Bachelor Programs

Studium Generale I

Course Code: DLBSG01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In the course "Studium Generale I", students deepen their knowledge in a self-selected subject area by completing an IU course outside their applicable curriculum. This gives them the opportunity to look beyond their own subject area and acquire further competencies. The associated option enables students to self-determine their study content to focus even more on issues relevant to them and/or to strengthen or develop selected competencies.

Course Outcomes

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Contents

- The course "Studium Generale I" offers students the opportunity to take courses outside of their curriculum and the result can be credited as an elective subject. In principle, all IU bachelor courses that fulfill the following requirements are creditable for this purpose:
  - They are not part of an integral part of the applicable mandatory curriculum.
  - They do not have admission requirements or students can prove that they have met the admission requirement.
- The examination of the selected courses must be taken in full and finally passed in order to be credited as part of the 'Studium Generale' .

Literature

Compulsory Reading

Further Reading

- See course description of the selected course

Study Format myStudies

Study Format	Course Type
myStudies	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods
see selected course

Study Format Distance Learning

Study Format	Course Type
Distance Learning	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods
See Selected Course

Studium Generale II

Course Code: DLBSG02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In the course "Studium Generale II", students deepen their knowledge in a self-selected subject area by completing an IU course outside their applicable curriculum. This gives them the opportunity to look beyond their own subject area and acquire further competencies. The associated option enables students to self-determine their study content to focus even more on issues relevant to them and/or to strengthen or develop selected competencies.

Course Outcomes

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Contents

- The course "Studium Generale II" offers students the opportunity to take courses outside of their curriculum and the result can be credited as an elective subject. In principle, all IU bachelor courses that fulfill the following requirements can be chosen for this purpose:
  - They are not part of an integral part of the applicable mandatory curriculum.
  - They do not have admission requirements or students can prove that they have met the admission requirement.
- The examination of the selected courses must be taken in full and finally passed in order to be credited as part of the 'Studium Generale' .

Literature

Compulsory Reading

Further Reading

- See course description of the selected course

Study Format Distance Learning

Study Format	Course Type
Distance Learning	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods
See Selected Course

Study Format myStudies

Study Format	Course Type
myStudies	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods

6. Semester

Business Intelligence

Module Code: DLBCSEBI

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Maik Drozdzynski (Business Intelligence) / Prof. Dr. Neil Arvin Bretana (Project: Business Intelligence)

Contributing Courses to Module

- Business Intelligence (DLBCSEBI01)
- Project: Business Intelligence (DLBCSEBI02)

Module Exam Type

Module Exam	Split Exam
	Business Intelligence • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Business Intelligence • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Business Intelligence

- Motivation and Conceptualization
- Data Provision
- Data Warehouse
- Modeling of Multidimensional Data Spaces
- Analysis Systems
- Distribution and Access

Project: Business Intelligence

Possible topics for the BI project include “Management of BI projects”, “Design of multidimensional data models” and “Prototypical implementation of small BI applications”.

Learning Outcomes

Business Intelligence

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Project: Business Intelligence

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology fields

Business Intelligence

Course Code: DLBCSEBI01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Business Intelligence (BI) is used to obtain information from company data that is relevant for targeted corporate management and the optimization of business activities. This course introduces and discusses techniques, procedures, and models for data provision, information generation, and analysis, as well the distribution of the information obtained. You will then be able to explain the various subject areas of data warehousing and independently select methods and techniques to meet specific requirements.

Course Outcomes

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Contents

1. Motivation and Conceptualization
   - 1.1 Motivation and Historical Development
   - 1.2 BI as a Framework
2. Data Provision
   - 2.1 Operative and Dispositive Systems
   - 2.2 The Data Warehouse Concept
   - 2.3 Architectural Variations
3. Data Warehouse
   - 3.1 ETL Process
   - 3.2 DWH and Data Mart
   - 3.3 ODS and Metadata
4. Modelling of Multidimensional Data Spaces

4.1 Data Modeling
4.2 OLAP Cubes
4.3 Physical Storage
4.4 Star and Snowflake Scheme
4.5 Historicization

5. Analysis Systems
5.1 Free Data Research and OLAP
5.2 Reporting Systems
5.3 Model-Based Analysis Systems
5.4 Concept-Oriented Systems

6. Distribution and Access
6.1 Information Distribution
6.2 Information Access

Literature

Compulsory Reading

Further Reading

- Grossmann, W., & Rinderle-Ma, S. (2015). Fundamentals of business intelligence. Springer.
- Sharda, R., Delen, D., & Turban, E. (2015). Business intelligence and analytics: Systems for decision support (10th ed.). Pearson.
- Sherman, R. (2014). Business intelligence guidebook: From data integration to analytics. Morgan Kaufmann.
- Vaisman, A., & Zimányi, E. (2022). Data warehouse systems: Design and implementation. Springer.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Business Intelligence

Course Code: DLBCSEBI02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using well-known methods and techniques from the field of Business Intelligence, students will work independently on a practical question in this course.At the end of the course you will be able to independently design and prototype Business Intelligence applications based on concrete requirements.

Course Outcomes

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Contents

- Implementation and documentation of practical questions regarding the use of Business Intelligence applications. Typical scenarios are, for example, “Management of BI projects”, “Design of multidimensional data models” and “Prototypical implementation of small BI applications”.

Literature

Compulsory Reading

Further Reading

- Liedtka, J. (2018). Why design thinking works. Harvard Business Review, 2018(9), 72–79.
- Meinel, C., & Leifer, L. J. (2021). Design thinking research: Interrogating the doing. Springer International Publishing.
- Meinel, C., Plattner, H., & Leifer, L. (2011). Design thinking: Understand – Improve – Apply. Springer Berlin Heidelberg.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Future Threats

Module Code: DLBCSEEFT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Jetzabel Maritza Serna Olvera (Threat Modeling) / N.N. (Project: Threat Modeling)

Contributing Courses to Module

- Threat Modeling (DLBCSEEFT01_E)
- Project: Threat Modeling (DLBCSEEFT02_E)

Module Exam Type

Module Exam	Split Exam
	Threat Modeling • Study Format "Distance Learning": Exam, 90 Minutes Project: Threat Modeling • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Threat Modeling

- Thinking C.I.A. and beyond
- Measuring the Cyber Threat
- Threat Modeling
- Attack libraries
- Rules, Regulations, and Law Enforcement
- Risk management
- Threat Mitigation

Project: Threat Modeling

This course covers the theory and practice of discovering and modeling threats in a given system, architecture or scenario. It covers common methodologies and sources for common threat patterns. In a project, the theory is translated to practice by analyzing a given situation for threats.

Learning Outcomes

Threat Modeling

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Project: Threat Modeling

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Threat Modeling

Course Code: DLBCSEEFT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01

Course Description

When a system or architecture is being created it is vital that possible threats are evaluated at the same time. By using both modeling methodologies and past observed attack patterns, it is possible to take a new or existing system and examine it for possible threats. With this analysis, possible risks and mitigations can be derived. While the most common methodologies are based on Attack Trees and the STRIDE model, recently attack modelling has also been using repositories of attacker techniques, tactics and procedures for inspiration.

Course Outcomes

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Contents

1. Thinking C.I.A. and beyond
    - 1.1 Confidentiality
    - 1.2 Integrity
    - 1.3 Availability
    - 1.4 Well-Known IT Security Issues
2. Measuring the Cyber Threat
    - 2.1 Concept of Threat Measuring
    - 2.2 Cyber Threat Metrics
    - 2.3 Measuring the Threat for an Organization
    - 2.4 Major Cyberattacks and their Impact
    - 2.5 Black Swan Events
3. Threat Modeling
    - 3.1 Attack Tree Methodology

- 3.2 STRIDE
- 3.3 DREAD
- 3.4 The Pyramid of Pain

4. Attack libraries
   - 4.1 CAPEC
   - 4.2 Solove's Taxonomy of Privacy
   - 4.3 Mitre ATT&CK®
   - 4.4 Identifying new Cyberattacks

5. Rules, Regulations, and Law Enforcement
   - 5.1 Cyber Laws
   - 5.2 Compliance and Law Enforcement

6. Risk management
   - 6.1 Risk Management: An Overview
   - 6.2 Incident Response and Crisis Management
   - 6.3 Unpredictable Events (Black Swan)
   - 6.4 Continuous Reevaluation

7. Threat Mitigation
   - 7.1 Cyber Defense Tactics and Techniques
   - 7.2 Risk Mitigation Strategies
   - 7.3 Validation of Defenses
   - 7.4 Security and Privacy by Design
   - 7.5 Implementing Threat Mitigation in an Organization

Literature
Compulsory Reading
Further Reading ▪ CAPEC: Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/ ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Mitre ATT&CK®. https://attack.mitre.org/ ▪ Pfleeger, C. P. / Pfleeger, S. L. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education. ▪ Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Threat Modeling

Course Code: DLBCSEEFT02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01, DLBCSEEFT01_E or DLBCSEEFT01_D

Course Description

Threats to modern computer systems are diverse and ever evolving. In this project, the student will have the opportunity to apply the art and science of threat modeling to a scenario to be defined by the instructor together with the student. The basis will be case studies, real or fictive, to which the student will be expected to identify and report on the threats using an appropriate methodology. This can be selected from methodologies such as Attack Trees, STRIDE, DREAD or a justified enumeration of CAPEC or Mitre ATT&CK® TTPs as the student feels most appropriate. The results will be presented as a report.

Course Outcomes

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Contents

- To a given case or scenario, the student will model the threats using one of the established methodologies and then submit the report and, if appropriate, any code and data. Specific problems and contexts will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Case Studies (Cyber): https://www.securitymagazine.com/topics/2664-case-studies-cyber
- Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS.
- Palmer, C. C. (2001): Ethical Hacking. In: IBM Systems Journal. 40 (3):769.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.
- Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (Security Controls in the Cloud) / Mohammad Reza Rostami (Project: Security by Design in the Cloud)

Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECS01_E)
- Project: Security by Design in the Cloud (DLBCSEECS02_E)

Module Exam Type

Module Exam	Split Exam
	Security Controls in the Cloud • Study Format "Duales myStudium": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Security Controls in the Cloud

- Cloud security
- Losing the intranet
- Security by design
- Secure cloud coding
- Confidentiality aspects
- Monitoring and Audit

Project: Security by Design in the Cloud

This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Learning Outcomes

Security Controls in the Cloud

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Project: Security by Design in the Cloud

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Security Controls in the Cloud

Course Code: DLBCSEECS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Contents

1. Cloud security is different
    - 1.1 Shared responsibility model
    - 1.2 Infrastructure as code
    - 1.3 The Private, Public and Hybrid Cloud
    - 1.4 Types of virtualization
    - 1.5 Cloud threat models: Mitre Cloud ATT&CK
2. Losing the intranet
    - 2.1 Identify and Access Management
    - 2.2 Principle of least privilege and fine-grained cloud access control
    - 2.3 Using Software Defined Networks, virtual private clouds and subnets
    - 2.4 Moving to a serverless architecture
    - 2.5 Defense in depth

3. Security by design
   - 3.1 Orchestration: Infrastructure as Code
   - 3.2 The Automate-Everything principle, Updating and Repeatability
   - 3.3 Reuse of good design patterns
   - 3.4 Container security
   - 3.5 Identification and Authentication

4. Secure cloud coding
   - 4.1 Software supply chain security
   - 4.2 Continuous Integration and Deployment
   - 4.3 Testing in code integration for security
   - 4.4 Canaries in code deployment
   - 4.5 Policy engines

5. Confidentiality aspects
   - 5.1 Secrets management
   - 5.2 Encryption of data at rest
   - 5.3 Encryption of data in transit
   - 5.4 Data leakage and exfiltration

6. Availability
   - 6.1 Storage tiers and locality
   - 6.2 Backup strategies
   - 6.3 Data and process redundancy
   - 6.4 Data lifecycle configuration
   - 6.5 DDoS mitigation

7. Locality
   - 7.1 Compliance requirements
   - 7.2 Geography of data/processes
   - 7.3 Redundancy of data centers
   - 7.4 Colocation for performance reasons

8. Monitoring and Audit
   - 8.1 Centralized logging
   - 8.2 Auditing orchestration scripts
   - 8.3 Detecting misconfigurations
   - 8.4 Cloud Forensics

9. Summary and Research topics
   - 9.1 Homomorphic encryption
   - 9.2 Attestation
   - 9.3 Proof-carrying data
   - 9.4 Side-channel attacks
   - 9.5 Conclusions

Literature

Compulsory Reading

Further Reading

- Mitre Cloud ATT&CK. https://attack.mitre.org/matrices/enterprise/cloud/

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E

Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Literature

Compulsory Reading

Further Reading

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Vulnerability Analysis and Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Enno Nagel (Principles of Ethical Hacking) / Prof. Dr. Björn Kaidel (Project: Pentesting)

Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEEPT01_E)
- Project: Pentesting (DLBCSEEPT02_E)

Module Exam Type

Module Exam	Split Exam
	Principles of Ethical Hacking • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes Project: Pentesting • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Principles of Ethical Hacking

- Introduction to Ethical Hacking
- Reconnaissance
- Enumeration and Vulnerability Analysis
- Hacking Systems
- Malware

Project: Pentesting

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.

Learning Outcomes

Principles of Ethical Hacking

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Project: Pentesting

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Contents

1. Introduction to Ethical Hacking
   - 1.1 Overview of Cyber Security
   - 1.2 Concepts of Cyber Kill Chain
   - 1.3 Hacking vs Ethical Hacking
   - 1.4 Laws and Standards
2. Reconnaissance
   - 2.1 Footprinting Techniques
   - 2.2 Network Scanning
   - 2.3 Host Discovery
   - 2.4 Service, Port and OS Discovery
   - 2.5 Scan beyond Security Measures
3. Enumeration and Vulnerability Analysis
   - 3.1 Enumeration Techniques
   - 3.2 Enumeration Countermeasures
   - 3.3 Vulnerability Assessment Techniques

- 3.4 Vulnerability Classification and Assessment

4. Hacking Systems
   - 4.1 Gaining Access to Systems
   - 4.2 Privilege Escalation
   - 4.3 Persistent Access
   - 4.4 Covering Traces

5. Malware
   - 5.1 Types of Malware
   - 5.2 Concepts of Fileless Malware
   - 5.3 Countermeasures

6. Sniffing
   - 6.1 Concepts of Sniffing
   - 6.2 Sniffing Techniques
   - 6.3 Countermeasures

7. Denial of Service
   - 7.1 Concepts of DoS/DDoS
   - 7.2 Attack Techniques
   - 7.3 Botnets
   - 7.4 Countermeasures

8. Social Engineering
   - 8.1 Concepts of Social Engineering
   - 8.2 Social Engineering Techniques
   - 8.3 Identity Theft and Impersonation
   - 8.4 Countermeasures

Literature
Compulsory Reading
Further Reading ▪ Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]). ▪ Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/ ▪ Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/ ▪ Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/ ▪ Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769. ▪ Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Pentesting

Course Code: DLBCSEEPT02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E

Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Industrial Systems Technology

Module Code: DLBCSEEIST_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Markus Kleffmann (Software Engineering Principles) / Dr. Rachel John Robinson (Internet of Things Security)

Contributing Courses to Module

- Software Engineering Principles (IGIS01_E)
- Internet of Things Security (DLBCSEEIST01_E)

Module Exam Type

Module Exam	Split Exam
	Software Engineering Principles • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Internet of Things Security • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Software Engineering Principles

- binary system
- Structure and function of computer systems
- Structure and function of communication networks
- Software life cycle
- Roles, phases, activities in software engineering

Internet of Things Security

Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Learning Outcomes

Software Engineering Principles

On successful completion, students will be able to

- perform simple calculations in the binary system (Boolean algebra).
- describe the structure of computer systems and communication networks.
- distinguish between the phases of a SW life cycle.
- distinguish roles and phases in the software process.
- know different process models of SW development.
- know typical challenges and risks of enterprise SW development.
- know different programming paradigms and their application.

Internet of Things Security

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Software Engineering Principles

Course Code: IGIS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of the course is to give students an insight into the technical and theoretical basics of software engineering. In addition to the general structure of computer systems, students are taught typical challenges in the development of enterprise information systems. Furthermore, the typical phases and activities in software engineering are presented to address these risks.

Course Outcomes

On successful completion, students will be able to

- perform simple calculations in the binary system (Boolean algebra).
- describe the structure of computer systems and communication networks.
- distinguish between the phases of a SW life cycle.
- distinguish roles and phases in the software process.
- know different process models of SW development.
- know typical challenges and risks of enterprise SW development.
- know different programming paradigms and their application.

Contents

1. Structure and organization of information systems
   - 1.1 0 and 1 as the basis of all IT systems
   - 1.2 Von Neumann Architecture
   - 1.3 Distributed systems and communication networks
   - 1.4 Enterprise information systems

2. Risks and challenges of enterprise software engineering
   - 2.1 Properties of enterprise software systems
   - 2.2 Software Engineering
   - 2.3 Risks and typical problems
   - 2.4 Root cause analysis
   - 2.5 Challenges in Software Engineering

3. Software life cycle: from planning to replacement
   - 3.1 The software life cycle at a glance

- 3.2 Planning
- 3.3 Development
- 3.4 Operation
- 3.5 Maintenance
- 3.6 Shutdown

4. Requirements engineering and specification
   - 4.1 requirements engineering
   - 4.2 Specification

5. Architecture and implementation
   - 5.1 Architecture
   - 5.2 Implementation

6. Testing, operation and evolution
   - 6.1 Testing
   - 6.2 Operation
   - 6.3 Evolution

7. Roles in Software Engineering
   - 7.1 Idea of the role-based approach
   - 7.2 Typical roles

8. Organization of software projects
   - 8.1 From process paradigm towards software process
   - 8.2 Process Paradigms

9. Software Process Frameworks
   - 9.1 V-model XT
   - 9.2 Rational Unified Process (RUP)
   - 9.3 Scrum

Literature
Compulsory Reading
Further Reading ▪ Pohl, K., & Rupp., C. (2015). Requirements engineering (2nd ed.). Rocky Nook. ▪ Sommerville, I. (2016). Software engineering (10th ed.). Pearson. ▪ Sommerville, I. (2019). Engineering software products: An introduction to modern software engineering. Pearson. ▪ Jacobson, I., Lawson, H., & Ng, P.-W. (2019). The essentials of modern software engineering. ACM Books.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Internet of Things Security

Course Code: DLBCSEEIST01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBINGEIT01_E or DLBINGEIT01

Course Description

Internet of Things (IoT) is a mega trend. It covers end consumer systems as well as industrial systems and technologies (Industrial IoT, or IIoT). There is an increasing amount of interconnected devices that composes the Internet of Things. In general, the Internet of Things architecture consists of terminal devices, cloud solutions and actors/sensors. Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Course Outcomes

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Contents

1. Basics of the Internet of Things (IoT)
   - 1.1 Introduction
   - 1.2 Architecture
   - 1.3 Non-Industrial Internet of Things
   - 1.4 Industry 4.0 (Industrial IoT)
2. Internet of Things Attacks
   - 2.1 Vulnerabilities, Threats and Risks
   - 2.2 Cyber Attacks and Countermeasures
3. Security by Design
   - 3.1 Project Management / Secure Development Life Cycle
   - 3.2 Static Testing
   - 3.3 Dynamic Testing
   - 3.4 DevSecOps

4. Securing Internet of Things Devices
   - 4.1 Security Risks
   - 4.2 Design Objectives

5. Operational Security
   - 5.1 Information and Cyber Security Management System
   - 5.2 Network Security
   - 5.3 Device Configuration
   - 5.4 Authentication and Authorization

6. Cloud Security
   - 6.1 Concept of the Fog
   - 6.2 Threats to Cloud Internet of Things Services
   - 6.3 Cloud-Based Security Services
   - 6.4 Securing the Cloud Solution

7. Big Data / Artificial Intelligence
   - 7.1 Supervised Learning
   - 7.2 Unsupervised Learning

Literature

Compulsory Reading

Further Reading

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum		WiSe/SoSe	English

Module Coordinator

Dr. Christian Prause (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01_E)
- Project: Defense against APTs (DLBCSEECTI02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Threat Feeds • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Project: Defense against APTs • Study Format "myStudies": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Attack Models and Threat Feeds

- Threat actors
- Modeling an Attack
- Attack Preparation TTPs
- Enterprise TTPs
- Industrial Control Systems TTPs
- Reporting

Project: Defense against APTs

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a "table top exercise" which data is already available and which extern threat feed data is required. After analyzing the "attack side" students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

Learning Outcomes

Attack Models and Threat Feeds

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Project: Defense against APTs

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a "table top exercise".
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Attack Models and Threat Feeds

Course Code: DLBCSEECTI01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data.It is rare that internal data is enough for a complete analysis and in practice the threat analysist must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience.After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Contents

1. Threat Actors
    - 1.1 Script Kiddies
    - 1.2 eCrime Threat Actors
    - 1.3 Advanced Persistent Threat Actors (APT)
    - 1.4 Threat Researchers
2. Modeling an Attack
    - 2.1 Phases of an Attack
    - 2.2 Lockheed Martin Kill-Chain
    - 2.3 Attack Trees
    - 2.4 Models for Security Risks and Cyber Attacks

3. Attack preparation TTPs
   - 3.1 Observability of Attack Preparations
   - 3.2 Operational Security of an Organization

4. Enterprise TTPs
   - 4.1 Behaviors of the Attacker
   - 4.2 Observable Data in an Enterprise

5. Industrial Control Systems TTPs
   - 5.1 Critical Infrastructure
   - 5.2 Special Considerations with IoT/ICS Defense

6. Threat data exchange
   - 6.1 Indicators of Compromise vs. Indicators of Attack
   - 6.2 Threat Intelligence Reports
   - 6.3 Ad-hoc Data Formats
   - 6.4 STIX Format, TAXII Protocol
   - 6.5 Semantics of Threat Data using Mitre ATT&CK, CVEs, etc.

7. Examples of Threat Analysis Platforms
   - 7.1 ACT Platform
   - 7.2 MISP
   - 7.3 OpenCTI

8. Examples of Threat Actors and their Modus Operandi
   - 8.1 Threat Model
   - 8.2 Relevant Indicator Data
   - 8.3 Relevant CTI Data
   - 8.4 Diagnosing the Threat
   - 8.5 Data Coverage Gap Analysis

9. Reporting
   - 9.1 Mapping Raw Data to Mitre ATT&CK
   - 9.2 Making Defensive Recommendations
   - 9.3 Writing Reports for Technical Staff
   - 9.4 Writing Reports for Management
   - 9.5 Working with Law Enforcement

Literature
Compulsory Reading
Further Reading ▪ Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. Retrieved from http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf ▪ Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2010). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved from https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LMWhite-Paper-Intel-Driven-Defense.pdf ▪ MISP Project. (n.d.). Retrieved from https://www.misp-project.org/ ▪ Mitre ATT&CK. (n.d.). Retrieved from https://attack.mitre.org/ ▪ Obrst, L., Chase, P., & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security. Fairfax, VA.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Defense against APTs

Course Code: DLBCSEECTI02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT´s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures.
To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT´s, ISP´s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a

comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT´s, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Mobile Threats

Module Code: DLBCSEEMT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Mohammad Reza Rostami (Wireless and Telecom Security) / Prof. Dr. Jörn-Marc Schmidt (Software Architectures of Mobile Devices)

Contributing Courses to Module

- Wireless and Telecom Security (DLBCSEEMT01_E)
- Software Architectures of Mobile Devices (DLBCSEEMT02_E)

Module Exam Type

Module Exam	Split Exam
	Wireless and Telecom Security • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes Software Architectures of Mobile Devices • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module
see curriculum

Module Contents

Wireless and Telecom Security

- Wireless protocols overview
- Wireless basics
- Telecom protocol classes
- Telecom architecture
- Handset and device security
- Threats
- Other wireless applications
- Protections

Software Architectures of Mobile Devices

- Handset technology stack
- Hardware
- Android operating system
- Apple iOS operating system
- Mobile devices
- Software ecosystems and security
- Mobile handset threats
- Mobile Device Management

Learning Outcomes

Wireless and Telecom Security

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Software Architectures of Mobile Devices

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Wireless and Telecom Security

Course Code: DLBCSEEMT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBIBRVS01_E or DLBIBRVS01; DLBCSEINF01_E or DLBCSEINF01_D

Course Description

The number of devices that can connect wirelessly to networks has already overtaken the number of desktop and laptop computers that connect to a local area network via a cable. In particular, phones and tablets dominate the market, and these connect to the wireless telecommunication networks. But there are also many other forms of wireless communication that devices use. The idiosyncrasies of these wireless systems need to be understood to integrate them in a complete security concept. Wireless protocols often force the user to trust in a system that they have no insights into and in this course, we will shine light onto the subject.

Course Outcomes

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Contents

1. Wireless protocols overview
   - 1.1 Personal area network protocols (Bluetooth, RFID, NFC, and more)
   - 1.2 Wireless local area network protocols (802.11a,b, g, ac , p and more)
   - 1.3 Wide area network protocols (Telecom protocols, LoRa, Satellite protocols, and more)
   - 1.4 Key exchange and cryptography in wireless networking
2. Wireless basics
   - 2.1 Frequencies
   - 2.2 Modulations
   - 2.3 Data Encodings
   - 2.4 Trade-offs
3. Telecom protocol classes

- 3.1 Telecom vs IT terminology and technologies
- 3.2 Telecom standards
- 3.3 Legacy digital protocols
- 3.4 LTE
- 3.5 5G

4. Telecom architecture
   - 4.1 Overall architecture
   - 4.2 Core architecture
   - 4.3 Software defined networking
   - 4.4 5G Campus Networks
   - 4.5 Application layer security

5. Handset and device security
   - 5.1 Requirements
   - 5.2 Typical hardware design
   - 5.3 IoT Devices

6. Threats
   - 6.1 Common attack vectors against devices and handsets
   - 6.2 Common attack vector against the core network
   - 6.3 Potential attacks against 5G campus networks

7. Other wireless applications
   - 7.1 Aviation and Nautical wireless protocols
   - 7.2 Proprietary device protocols
   - 7.3 Wide area sensor networks (LoRa, Sigfox, ...)
   - 7.4 Digital voice/data technologies (DECT/GAP, TETRA, ...)
   - 7.5 Satellite communications

8. Protections
   - 8.1 Integrating mobile technology securely
   - 8.2 Monitoring mobile devices

Literature
Compulsory Reading
Further Reading ▪ Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G. ▪ Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187. ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Software Architectures of Mobile Devices

Course Code: DLBCSEEMT02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Mobile devices have supplanted desktops and laptops as the most common end-user device. The smart phone has become a central business tool. Users run their entire lives from them. Furthermore, the Internet of Things are also using these mobile platforms. But too often, the risks and opportunities associated with these mobile devices are opaque to the security administrators in particular as these devices often operate outside the traditional Intranet. In this course, we examine how the dominant players, Android and Apple iOS, handle security in their software stack and ecosystem. We also look at the overlooked problem of IoT Security and wrap up with organizational solutions.

Course Outcomes

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Contents

1. Handset technology stack
    - 1.1 Hardware
    - 1.2 Firmware
    - 1.3 Operating system
    - 1.4 Applications
    - 1.5 Ecosystem
2. Hardware
    - 2.1 RF modules
    - 2.2 PDA module
    - 2.3 Trusted Execution Environment component
    - 2.4 Biometric devices
    - 2.5 Location technology

3. Android operating system
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel and Hardware abstraction layer
   - 3.4 Sandboxing and virtualization
   - 3.5 Code signing

4. Apple iOS operating system
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel and Frameworks
   - 4.4 Sandboxing and virtualization
   - 4.5 Code signing

5. Mobile devices
   - 5.1 The Internet of things
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android on devices
   - 5.5 Other common embedded operating systems

6. Software ecosystems and security
   - 6.1 Google play
   - 6.2 Apple store
   - 6.3 Security providers
   - 6.4 The role of the Cloud

7. Mobile handset threats
   - 7.1 Historic examples of handset attacks
   - 7.2 Taxonomy of Handset threats
   - 7.3 Jailbreaking

8. Mobile Device Management
   - 8.1 The threats of BYOD
   - 8.2 Unique threats to mobile devices
   - 8.3 Patch and policy management

Literature
Compulsory Reading
Further Reading ▪ Gupta, A. (2014): Learning Pentesting for Android Devices ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ N.A. (2020): Android Enterprise Security White Paper. ▪ N.A. (2019): iOS Security iOS 12.3. https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf ▪ Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Study Format myStudies

Study Format	**Course Type**
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Studium Generale III and IV

Module Code: DLBSGDUV_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	None	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Studium Generale III) / N.N. (Studium Generale IV)

Contributing Courses to Module

- Studium Generale III (DLBSG03_E)
- Studium Generale IV (DLBSG04_E)

Module Exam Type

Module Exam	Split Exam
	Studium Generale III • Study Format "Distance Learning": See Selected Course Studium Generale IV • Study Format "Distance Learning": See Selected Course

Weight of Module

see curriculum

Module Contents

Studium Generale III

In principle, all IU bachelor courses can be selected as courses for the "Studium Generale", so that the content can be chosen from the entire breadth of the IU distance learning program.

Studium Generale IV

In principle, all IU bachelor courses can be selected as courses for the "Studium Generale", so that the content can be chosen from the entire breadth of the IU distance learning program.

Learning Outcomes

Studium Generale III

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Studium Generale IV

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Links to other Modules within the Study Program	Links to other Study Programs of the University
It is a stand-alone offering with possible references to various required and elective modules	All IU Distance Learning Bachelor Programs

Studium Generale III

Course Code: DLBSG03_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	None

Course Description

In the course "Studium Generale III", students deepen their knowledge in a self-selected subject area by completing an IU course outside their applicable curriculum. This gives them the opportunity to look beyond their own subject area and acquire further competencies. The associated option enables students to self-determine their study content to focus even more on issues relevant to them and/or to strengthen or develop selected competencies.

Course Outcomes

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Contents

- The course "Studium Generale III" offers students the opportunity to take courses outside of their curriculum and the result can be credited as an elective subject. In principle, all IU bachelor courses that fulfill the following requirements can be chosen for this purpose:
  - They are not part of an integral part of the applicable mandatory curriculum.
  - They do not have admission requirements or students can prove that they have met the admission requirement.
- The examination of the selected courses must be taken in full and finally passed in order to be credited as part of the 'Studium Generale' .

Literature

Compulsory Reading

Further Reading

- See course description of the selected course

Study Format Distance Learning

Study Format	Course Type
Distance Learning	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods

Studium Generale IV

Course Code: DLBSG04_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	None

Course Description

In the course "Studium Generale IV", students deepen their knowledge in a self-selected subject area by completing an IU course outside their applicable curriculum. This gives them the opportunity to look beyond their own subject area and acquire further competencies. The associated option enables students to self-determine their study content to focus even more on issues relevant to them and/or to strengthen or develop selected competencies.

Course Outcomes

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- to deepen one's own skills and abilities in a self-directed manner.
- to look beyond the boundaries of their own area of expertise.

Contents

- The course "Studium Generale IV" offers students the opportunity to take courses outside of their curriculum and the result can be credited as an elective subject. In principle, all IU bachelor courses that fulfill the following requirements can be chosen for this purpose:
  - They are not part of an integral part of the applicable mandatory curriculum.
  - They do not have admission requirements or students can prove that they have met the admission requirement.
- The examination of the selected courses must be taken in full and finally passed in order to be credited as part of the 'Studium Generale' .

Literature

Compulsory Reading

Further Reading

- See course description of the selected course

Study Format Distance Learning

Study Format	Course Type
Distance Learning	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods

IT Security Consulting

Module Code: DLBCSEEISC_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Rachel John Robinson (Technical and Operational IT Security Concepts) / Jetzabel Maritza Serna-Olvera (Project: Configuration and Application of SIEM Systems)

Contributing Courses to Module

- Technical and Operational IT Security Concepts (DLBCSEEISC01_E)
- Project: Configuration and Application of SIEM Systems (DLBCSEEISC02_E)

Module Exam Type

Module Exam	Split Exam
	Technical and Operational IT Security Concepts • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Configuration and Application of SIEM Systems • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Technical and Operational IT Security Concepts

- Network analysis and evaluation
- Protection Profiles
- Intrusion Detection Systems
- Network Monitoring
- Security Information and Event Management (SIEM)
- IT-Security evaluation and assessment

Project: Configuration and Application of SIEM Systems

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) Tool into an Enterprise IT-Environment. Students will need to consider practical aspects such as different data sources, data fusion and big data analytics methods and processing, as well as constraints such as data availability and multiple data formats.

Learning Outcomes

Technical and Operational IT Security Concepts

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Project: Configuration and Application of SIEM Systems

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Technical and Operational IT Security Concepts

Course Code: DLBCSEEISC01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-Systems and Networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructure require higher security mechanism regarding confidentiality, integrity and availability. Based on specific “Protection Profiles” high sophisticated tools, mechanisms and procedures need to be designed, implemented, configurated and operated.With this course the student will be able to evaluate given IT-Infrastructure, support the security-design of new IT-Systems and Networks by developing specific Protection Profiles, evaluate which technical and operational security measures and application are required and how these are integrated, configured and operated.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Contents

1. Network Analysis and Evaluation
    - 1.1 Layer Specific Threats and Vulnerabilities
    - 1.2 DATA Flow, Interdependencies and Interrelationships
    - 1.3 Vulnerability Scanning and Detection
    - 1.4 Supporting Tools and Techniques
2. Protection Profiles
    - 2.1 Reference Architecture Technology and Networking
    - 2.2 Risk Assessment, Residual Risk and Risk Management
    - 2.3 Security Requirements and Safeguards
    - 2.4 Security Evaluation of IT-Security Products

2.5 Accreditation of IT-Systems and Networks

3. Intrusion Detection Systems
   - 3.1 Detection Strategy
   - 3.2 Data Sources, Sensors
   - 3.3 Analytics
   - 3.4 Indicators of Compromise

4. Network Monitoring
   - 4.1 Threat Protection Systems
   - 4.2 Wireless Sensor Networks Technology
   - 4.3 Threat Information Sharing

5. Security Information and Event Management (SIEM)
   - 5.1 Technical and Operational DATA Sources
   - 5.2 DATA Fusion
   - 5.3 Network Norm Behavior
   - 5.4 Big Data Analysis – Transferring Technical Data for Operational Information
   - 5.5 Security Situation Picture, Situational Awareness
   - 5.6 Incident Response Strategies and Automated Responses

6. IT-Security Evaluation and Assessment
   - 6.1 IT-Security Metrics
   - 6.2 IT-Security Assessment

Literature

Compulsory Reading

Further Reading

- Federal Office for Information Security (BSI) (2018): IT-Grundschutz Profiles - Structural Description - COMMUNITY DRAFT.
- Hayden, L. (2010): IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education.
- McNab, C. (2016): Network Security Assessment: Know Your Network. 3. Auflage, O'Reilly UK Ltd.
- Miller, D. R. et al. (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Configuration and Application of SIEM Systems

Course Code: DLBCSEEISC02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEEISC01_E or DLBCSEEISC01_D

Course Description

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) Tool into an Enterprise IT-Environment. Students will need to consider practical aspects such as different data sources, data fusion and big data analytics methods and processing, as well as constraints such as data availability and multiple data formats. Furthermore, students will face the challenge to transfer technical data into operational Information to initiate valid responses. By the end of this course, students will have obtained well-founded knowledge of the integration of SIEM into enterprise IT infrastructure, applications and services.

Course Outcomes

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Contents

- This course focuses on practical aspects of the implementation of a SIEM into an enterprise IT infrastructure environment. Students start with a chosen use case and SIEM and then evaluate requirements which need to be fulfilled so that the SIEM can be used as part of an enterprise IT system / network. Students need to evaluate requirements for sensors, network monitoring, intrusion detection, data fusion, big data analytics, and translating technical data into operational information.
- Based on the available information, valid responses – including automated responses - will be identified and processed.
- All relevant artifacts and considerations are documented by the students in a project report.

Literature
Compulsory Reading
Further Reading ▪ Al-Sakib, K. P. (2016): The State of the Art in Intrusion Prevention and Detection. Routledge, Abingdon. ▪ Miller, D. et al (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY. ▪ Mitchell, H. B. (2007): Multi-Sensor Data Fusion: An Introduction. Springer Verlag, Berlin.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Social Engineering

Module Code: DLBCSEESE_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Social Engineering and Insider Threats) / N.N. (Project: Social Engineering)

Contributing Courses to Module

- Social Engineering and Insider Threats (DLBCSEESE01_E)
- Project: Social Engineering (DLBCSEESE02_E)

Module Exam Type

Module Exam	Split Exam
	Social Engineering and Insider Threats • Study Format "myStudies": Written Assessment: Case Study • Study Format "Distance Learning": Written Assessment: Case Study Project: Social Engineering • Study Format "myStudies": Oral Project Report • Study Format "Distance Learning": Oral Project Report

Weight of Module

see curriculum

Module Contents

Social Engineering and Insider Threats

- Social Engineering Methods
- Legal Aspects of Social Engineering
- Insider Threat Detection
- Security Policies and Regulations
- National and International Cooperation and Information Exchange

Project: Social Engineering

This course focuses on practical aspects to prevent, detect and recover from socialengineering driven attacks as well as threat deriving from hostile insiders.

Learning Outcomes

Social Engineering and Insider Threats

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Project: Social Engineering

On successful completion, students will be able to

- recognize the importance of the “Human Factor” in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Social Engineering and Insider Threats

Course Code: DLBCSEESE01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-systems and networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructures are of high interest for attackers to gain information (Cyber Espionage) to manipulate or destroy information and data as well as interrupt basic functions and services by compromising these systems and enterprises. One attack vector is targeted to the users and operators to misuse these people as workforce to break security policies and regulations. Social Engineering or social manipulation is widely used by adversaries to gain the necessary information to compromise IT-Infrastructures and to achieve their specific goals. Using methods of social engineering is very close to the so called “Insider Threat”. People from inside the organization act for various reasons against the security policies and regulations of their own enterprise. Revenge, dissatisfaction or sometimes criminal intent are reasons for such behavior. A combination of social engineering and “hostile insiders” is a gold nugget for all adversaries. Therefore, technical and organizational measures have to be developed and implemented to avert such threats. With this course, students will be able to recognize methods of social engineering and identify insider threats. They will be able to develop and implement preventive security policies and regulations as well as responsive security measures to counter these threats.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Contents

1. Social Engineering Methods

- 1.1 Phishing, Spear Phishing and Dynamite Phishing
- 1.2 Quid pro quo, Baiting, Media Dropping
- 1.3 Scareware, CEO-Fraud
- 1.4 Pretexting, Tailgating

2. Legal Aspects of Social Engineering
   - 2.1 Compliance, Code of Conduct
   - 2.2 Identity Theft
   - 2.3 Data Privacy

3. Insider Threat Detection
   - 3.1 Data Mining Techniques
   - 3.2 Application of Machine Learning Methods
   - 3.3 Comprehensive Framework for Insider Threat Detection and Response
   - 3.4 Self-assessment Tools for Evaluation
   - 3.5 Organizational Countermeasures and Awareness

4. Security Policies and Regulations
   - 4.1 Organizational Framework, Compliance, Code of Conduct
   - 4.2 Training and Awareness
   - 4.3 Protection of sensitive Information
   - 4.4 Security Monitoring and Incident Response

5. National and International Cooperation and Information Exchange
   - 5.1 Cooperation with Internet Service Providers (ISP) and IT-Security stakeholders
   - 5.2 Exchange Platforms and Forums for Tactics Techniques and Procedures (TTP´s) and Best Practices
   - 5.3 Cooperation with National Security Authorities

Literature
Compulsory Reading
Further Reading ▪ Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited. ▪ Company: TrustedSec. (Internet DEMO Version to subscribe) ▪ Robert W. Gehl; Sean T Lawson (2022): Social Engineering : How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication. Online verfügbar unter https://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=2932693&site=eds-live. ▪ Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann. ▪ Kennedy, D.: The Social-Engineer Toolkit (SET)

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Project: Social Engineering

Course Code: DLBCSEESE02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEESE01_E or DLBCSEESE01_D

Course Description

This project course will give students hands-on experience in the challenging task to prevent and counter social engineering attacks and eliminate or as a minimum mitigate the insider threat to the Enterprise IT-Systems and Networks. Students will need to consider practical aspects of social and psychological challenges – the so called "Human Factor" - as well as the application of technical toolkits to detect attacks driven by social engineering methods or caused by hostile insiders. Through this course Students will develop a complete overview of organizational, technical and procedural measures by analyzing the threat vector landscape, identify vulnerabilities and security gaps in the enterprise and develop and implement practical security policies and regulations, including security awareness campaigns, to prevent and recover from incidents caused by social engineering and insider threats.

Course Outcomes

On successful completion, students will be able to

- recognize the importance of the "Human Factor" in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Contents

- This project course focuses on practical aspects to prevent, detect and recover from social engineering driven attacks as well as threat deriving from hostile insiders. Students start with a chosen use case to analyze a tangible and successful social engineering campaign, identify the main attack vectors and learn how different activities on multiple levels concur to reach the objective or the attacker. Students need to analyze the security framework of the attacked enterprise, identify the vulnerability gaps and shortfalls that allowed the social engineering attack to be successful. Taking into account the "Human Factor" the students

will then develop organizational and technical security policies to show how a specific attack could have been prevented and the damage been avoided or mitigated. All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature
Compulsory Reading
Further Reading ▪ Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane. ▪ Company: TrustedSec. (Internet DEMO Version to subscribe) ▪ Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford. ▪ Kennedy, D.: The Social-Engineer Toolkit (SET)

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Mohammad Reza Rostami (Static and Dynamic Malware Analysis) / N.N. (Seminar: Sandbox Interpretation)

Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02_E)

Module Exam Type

Module Exam	Split Exam
	Static and Dynamic Malware Analysis • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "myStudies": Written Assessment: Research Essay • Study Format "Duales myStudium": Written Assessment: Research Essay • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module
see curriculum

Module Contents

Static and Dynamic Malware Analysis

- Objectives in Malware analysis
- Analysis Lab setup
- Tools of the trade
- Malware Classification
- Sandboxes
- Reversing
- Digging deeper

Seminar: Sandbox Interpretation

This course is about the practical application of Malware analysis techniques to real sandbox log files.

Learning Outcomes

Static and Dynamic Malware Analysis

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Seminar: Sandbox Interpretation

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Malware is a top compromise vector in cyber attacks. Analyzing the attacking Malware gives the security analyst insights into the methodology and intension of the attacker. There are a number of ways that Malware can be analyzed and this course will introduce the most common ones.

Course Outcomes

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Contents

1. Objectives in Malware Analysis
   - 1.1 Understanding Malware: Components, Types, and Analysis
   - 1.2 Forensics
   - 1.3 Root Cause Analysis
   - 1.4 The MITRE Attack Framework
   - 1.5 Best Practices for Malware Prevention and Mitigation
2. Analysis Lab Setup
   - 2.1 Building a Secure Malware Analysis Lab
   - 2.2 Stealth
   - 2.3 Isolation
   - 2.4 Honeypots
3. Tools of the Trade
   - 3.1 Virtual Machines
   - 3.2 Debugger
   - 3.3 Anti Debugging Mechanism
   - 3.4 Disassembler

4. Malware Classification
   - 4.1 Malware Triage and Classification
   - 4.2 Structure of a Virus
   - 4.3 Antivirus
   - 4.4 VirusTotal
   - 4.5 Yara
   - 4.6 AI-assisted Malware Analysis

5. Sandboxes
   - 5.1 Different Sandbox Concepts and Their Purposes
   - 5.2 Levels of Interaction
   - 5.3 Instrumentation
   - 5.4 Online Sandboxing Services
   - 5.5 Sandbox Detection and Evasion

6. Reversing
   - 6.1 Understanding Malware Analysis and Its Impact
   - 6.2 Unpacking, Decrypting, and De-Obfuscation
   - 6.3 Debugging Techniques
   - 6.4 Control Flow Analysis
   - 6.5 Library and System Calls

7. Digging Deeper
   - 7.1 Threat Intelligence Integration
   - 7.2 Analysis of JavaScript Code
   - 7.3 Memory Forensics
   - 7.4 Understanding and Debugging Rootkits

Literature

Compulsory Reading

Further Reading

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing.
- Mitre ATT&CK®. https://attack.mitre.org/
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: https://beginners.re/ (last accessed: 24 August 2020)

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	**Course Type**
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E

Course Description

In this course, we explore the most important tool in Malware analysis, the Sandbox and extract from the Sandbox logs the potential attacks exhibited by the Malware.

Course Outcomes

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Contents

- This course is about the practical application of Malware analysis techniques to real sandbox log files and extract the indicators of compromise and Malware objectives into a report.

Literature

Compulsory Reading

Further Reading

- Gregg, M. (2008): Build Your Own Security Lab: A Field Guide for Network Testing. Wiley, Hoboken, NJ.
- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.

Study Format myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

DevSecOps

Module Code: DLBCSEEDSO_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Jörn Fahsel (Techniques and methods for agile software development) / N.N. (Project: Agile DevSecOps Software Engineering)

Contributing Courses to Module

- Techniques and methods for agile software development (IWNF01_E)
- Project: Agile DevSecOps Software Engineering (DLBCSEEDSO01_E)

Module Exam Type

Module Exam

Split Exam

Techniques and methods for agile software development

- Study Format "myStudies": Exam, 90 Minutes
- Study Format "Distance Learning": Exam, 90 Minutes

Project: Agile DevSecOps Software Engineering

- Study Format "Distance Learning": Written Assessment: Project Report
- Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Techniques and methods for agile software development

- Characteristics and Principles of Agility
- Agility in Small Teams with SCRUM
- Agile Project Management
- Agile Requirements and Software Architecture Management
- Agile Testing
- Agile Delivery and Deployment

Project: Agile DevSecOps Software Engineering

This module provides the fundamental security principles for leveraging DevOps in software engineering, also known as the DevSecOps paradigm. Given a security-relevant scenario, this module will illustrate good DevSecOps practices like definition of security baselines, threat modelling approaches, and security automation as part of the continuous integration/continuous development (CI/CD) pipeline.

Learning Outcomes

Techniques and methods for agile software development

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Project: Agile DevSecOps Software Engineering

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Techniques and methods for agile software development

Course Code: IWNF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The goal of the course is to give students a deeper insight into the topic of agile software development. First of all, the basic characteristics and principles of agility are presented and discussed. Afterwards, it is shown how small projects and teams can use agile software engineering and how agile principles can be transferred and applied to large projects. Afterwards, agile techniques are taught for selected core activities in software engineering, with a focus on testing, delivery and deployment.

Course Outcomes

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Contents

1. Characteristics and Principles of Agility
   - 1.1 Features and Challenges of Software Projects
   - 1.2 Classification of Uncertainty
   - 1.3 Comparison of Agile and Classic Software Development
   - 1.4 Principles of Agility
2. Agility in Small Teams with Scrum
   - 2.1 Basics of SCRUM
   - 2.2 Central Management Artifact: Product Backlog
   - 2.3 Other Management Artifacts abd Tools
3. Agile Project Management
   - 3.1 Planning Levels in Agile Project Management

3.2 Agile Portfolio Management
3.3 Organization of Several Teams in One Project
3.4 Product and Release Planning

4. Agile Requirements and Software Architecture Management
4.1 Requirements Engineering in Agile Projects
4.2 Architecture Management in Agile Projects

5. Agile Testing
5.1 Basic Principles and Requirements for the Quality Assurance Organization
5.2 Test Levels and Agility
5.3 Test Automation

6. Agile Delivery and Deployment
6.1 Continuous Delivery Pipeline
6.2 Continuous Build and Continuous Integration
6.3 Acceptance Tests, Load Tests and Continuous Deployment

Literature

Compulsory Reading

Further Reading

- Biffl, S. et al. (Hrsg.) (2005): Value-Based Software Engineering. Springer, Berlin/Heidelberg.
- Highsmith, J. (2009): Agile Project Management: Creating Innovative Products. Addison Wesley, Upper Saddle River, NJ.
- Layton, M. C. (2012): Agile project management for dummies. John Wiley & Sons, New York, NY.
- Rubin, K. S. (2012): Essential Scrum: A Practical Guide to the Most Popular Agile Process. Addison Wesley, Upper Saddle River, NJ.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Agile DevSecOps Software Engineering

Course Code: DLBCSEEDSO01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	IWNF01_E or DLBWIWTMAS01

Course Description

This course covers the basic security principles for leveraging the DevSecOps approach in software engineering scenarios. The content of this course will illustrate the adoption of DevSecOps to continuously and holistically improve the security of an organization, rather than just focusing on protecting the underlying software infrastructure (as in the case of traditional non-agile methodologies). By presenting DevSecOps principles like threat modelling, definition of security baselines, security automation/tools, and continuous compliance monitoring, this course will teach how security can be integrated while developing a software engineering product.

Course Outcomes

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Contents

- Despite the broad adoption of DevOps in the industry, the integration of security principles into this paradigm (i.e., DevSecOps) is still an open challenge for many practitioners. In this course the students will learn fundamental DevSecOps concepts like threat modelling, definition of security baselines, continuous compliance monitoring, and integration of security automation in DevOps.

Literature
Compulsory Reading
Further Reading ▪ Johnson, E. (2020): Secure DevOps. A Practical Introduction. (URL: https://www.sans.org/ondemand/course/secure-dev-ops-a-practical-introduction [Retrieved: 15.08.2020]). ▪ Hsu, T. (2018): Hands-On Security in DevOps. Packt Publishing, UK. ▪ Microsoft. (2020): Secure DevOps. Making security principles and practices an integral part of DevOps while maintaining improved efficiency and productivity. (URL: https://www.microsoft.com/en-us/securityengineering/devsecops [Retrieved: 15.08.2020]). ▪ Schneider, C. (2015): Security DevOps. Staying secure in agile projects. (URL: https://owaspappseceurope2015.sched.com/event/378l/security-devops-staying-secure-in-agile-projects [Retrieved: 15.08.2020]). ▪ Yasar, H. (2016): An Introduction to Secure DevOps. Including Security in the Software Lifecycle. (URL: https://insights.sei.cmu.edu/devops/2016/11/an-introduction-to-secure-devops-including-security-in-the-software-lifecycle.html [Retrieved: 15.08.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Security in Complex Networks

Module Code: DLBCSEESCN_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Claudia Heß (IT Architecture Management) / Prof. Dr. Holger Klus (Project: IT Security Architecture)

Contributing Courses to Module

- IT Architecture Management (DLBCSEITPAM02)
- Project: IT Security Architecture (DLBCSEESCN01_E)

Module Exam Type

Module Exam	Split Exam
	IT Architecture Management • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: IT Security Architecture • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

IT Architecture Management

- Basic terms and foundations of IT enterprise architectures management
- IT application portfolio management
- Architecture governance
- Modeling of IT enterprise architectures
- Frameworks using TOGAF as an example
- Reference models and sample catalogues

Project: IT Security Architecture

Using well-known methods and techniques from the field of IT architecture management, students will be able to develop a well-grounded overview of IT-infrastructure regarding IT-strategy and strategic management. Students will understand and take advantage of typical concepts, methods and models for all tasks in the framework of architecture management. Emphasis will be taken to the security aspects of the IT infrastructure by designing and implementing IT-security architecture in the overall framework.

Learning Outcomes

IT Architecture Management

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Project: IT Security Architecture

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

IT Architecture Management

Course Code: DLBCSEITPAM02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In addition to concrete IT projects, such as the development of a new IT system or the introduction of standard software, a strategic management system for organizational-wide IT infrastructure – that is, for all IT hardware and software systems – must be used.Strategic management is the responsibility of the IT enterprise architect, who operates IT architecture management. Their task is to strategically align IT infrastructure with an organization's business and IT strategy.This course covers the typical concepts, methods, procedures, and IT models of architecture management.

Course Outcomes

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Contents

1. Basic Terms and Foundation for the Management of IT Enterprise Architectures
   - 1.1 IT Enterprise Architecture
   - 1.2 Goals of Enterprise Architecture Management
   - 1.3 Processes in the Management of IT Enterprise Architectures
2. IT Application Portfolio Management
   - 2.1 IT Application Portfolio Management Overview
   - 2.2 Application Manual
   - 2.3 Portfolio Analysis
   - 2.4 Development Planning
3. Architecture Governance

3.1 Organizational Structure
3.2 Policy Development and Enforcement
3.3 Project Support

4. Modeling of IT Enterprise Architectures
   4.1 Models in the Context of IT Architecture Management
   4.2 Forms of Documentation for Processes and Applications
   4.3 Forms of Documentation for Systems and Technologies

5. Frameworks Using the Example of TOGAF
   5.1 Fundamentals and Use of IT Architecture Frameworks
   5.2 Overview and Categories of EAM Frameworks
   5.3 The Open Group Architecture Framework (TOGAF)

6. Reference Models and Sample Catalogues
   6.1 Architecture Reference Models
   6.2 EAM Design Sample Catalogue

Literature

Compulsory Reading

Further Reading

- Ahlemann, F., Messerschmidt, M., Stettiner, E., & Legner, C. (2012). Strategic enterprise architecture management. Challenges, best practices, and future developments. Springer-Verlag.
- Perroud, T., & Inversini, R. (2013). Enterprise architecture patterns: Practical solutions for recurring IT-architecture problems. Springer.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: IT Security Architecture

Course Code: DLBCSEESCN01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEITPAM02 or IAMG01

Course Description

Using methods and techniques from the field IT architecture management, students will work independently on a practical question of IT security architecture. By the end of this course students will be able to independently develop IT security architecture models, based on an existing IT-system / network architecture.

Course Outcomes

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Contents

- Implementation and documentation of practical questions regarding IT security in the framework of IT architecture management. Typical scenarios are, for example, “Implementation of IT security devices in complex networks”, “Design of processes for security updates and patch management” and “using in-house resources or outsourcing of IT security tasks”.

Literature
Compulsory Reading
Further Reading ▪ Calder, Alan. (2020). Cyber Security - Essential Principles to Secure Your Organisation. IT Governance Publishing. ▪ Dr. Erdal Ozkaya (2019): Cybersecurity: The Beginner's Guide: A Comprehensive Guide to Getting Started in Cybersecurity. ▪ Pierre Bernard (2012): COBIT® 5 - A Management Guide. Online verfügbar unter https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1558038&site=eds-live. ▪ Virgilio Viegas; Oben Kuyucu (2022): IT Security Controls: A Guide to Corporate Standards and Frameworks.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Slides	☑ Guideline

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Mohammad Reza Rostami (Protocols, Log- and Dataflow-Analysis in Depth) / Dr. Jetzabel Maritza Serna-Olvera (Seminar: Threat Hunting, Analysis and Incident Response)

Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02_E)

Module Exam Type

Module Exam

Split Exam

Protocols, Log- and Dataflow-Analysis in Depth

- Study Format "Duales myStudium": Exam, 90 Minutes
- Study Format "myStudies": Exam, 90 Minutes
- Study Format "Distance Learning": Exam, 90 Minutes

Seminar: Threat Hunting, Analysis and Incident Response

- Study Format "Duales myStudium": Written Assessment: Research Essay
- Study Format "Distance Learning": Written Assessment: Research Essay
- Study Format "myStudies": Written Assessment: Research Essay

Weight of Module
see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Network Basics
- Operating System Logs
- Packet Capturing and Analysis
- Log Management
- Preparation for Attacks
- Intrusion Detection and Prevention System

Seminar: Threat Hunting, Analysis and Incident Response

- Mitre ATT&CK TTPs
- APT actors
- Security coverage gap analysis

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Seminar: Threat Hunting, Analysis and Incident Response

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Contents

1. Introduction to Network Forensics
    - 1.1 Basics of Network Forensics
    - 1.2 Evidence Handling Standards
    - 1.3 Verification of Evidence
2. Network Basics
    - 2.1 Protocol Basics and Functionality
    - 2.2 Difference between the OSI Model and TCP/IP Architecture
    - 2.3 Basics of TCP and UDP including Ports and Protocols
    - 2.4 DNS, DHCP and ARP
3. Host-Side Artifacts
    - 3.1 Network-based Artifacts stored in the Operating Systems
    - 3.2 Services and Ports
    - 3.3 TCP Connection States
    - 3.4 Tools for extracting the Artifacts

4. Packet Capture and Analysis
   - 4.1 Capturing Packets
   - 4.2 Tools like TCPDump and Wireshark
   - 4.3 Analysis of captured Packets

5. Location Information
   - 5.1 Impact of Time Zones on Investigations
   - 5.2 Location Information from the Network
   - 5.3 Location-based Services with Web Applications
   - 5.4 Location Information from WiFi

6. Preparing for Attacks
   - 6.1 Manage Netflow Data
   - 6.2 Loggings
   - 6.3 Antivirus
   - 6.4 SIEM and Incident Response

7. Intrusion Detection and Prevention Systems
   - 7.1 Detection Styles
   - 7.2 Host-based versus Network-based
   - 7.3 Challenges with Intrusion Detection and Prevention Systems
   - 7.4 Firewall and Application Logs

8. Correlation of Data
   - 8.1 Synchronization of Time across Multiple Systems
   - 8.2 Log Aggregation and Management
   - 8.3 Importance of Timelines

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- NIST Special Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Business Intelligence

Module Code: DLBCSEBI

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Maik Drozdzynski (Business Intelligence) / Prof. Dr. Neil Arvin Bretana (Project: Business Intelligence)

Contributing Courses to Module

- Business Intelligence (DLBCSEBI01)
- Project: Business Intelligence (DLBCSEBI02)

Module Exam Type

Module Exam

Split Exam

Business Intelligence

- Study Format "myStudies": Exam, 90 Minutes
- Study Format "Distance Learning": Exam, 90 Minutes

Project: Business Intelligence

- Study Format "Distance Learning": Written Assessment: Project Report
- Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Business Intelligence

- Motivation and Conceptualization
- Data Provision
- Data Warehouse
- Modeling of Multidimensional Data Spaces
- Analysis Systems
- Distribution and Access

Project: Business Intelligence

Possible topics for the BI project include “Management of BI projects”, “Design of multidimensional data models” and “Prototypical implementation of small BI applications”.

Learning Outcomes

Business Intelligence

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Project: Business Intelligence

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology fields

Business Intelligence

Course Code: DLBCSEBI01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Business Intelligence (BI) is used to obtain information from company data that is relevant for targeted corporate management and the optimization of business activities. This course introduces and discusses techniques, procedures, and models for data provision, information generation, and analysis, as well the distribution of the information obtained. You will then be able to explain the various subject areas of data warehousing and independently select methods and techniques to meet specific requirements.

Course Outcomes

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Contents

1. Motivation and Conceptualization
   - 1.1 Motivation and Historical Development
   - 1.2 BI as a Framework
2. Data Provision
   - 2.1 Operative and Dispositive Systems
   - 2.2 The Data Warehouse Concept
   - 2.3 Architectural Variations
3. Data Warehouse
   - 3.1 ETL Process
   - 3.2 DWH and Data Mart
   - 3.3 ODS and Metadata
4. Modelling of Multidimensional Data Spaces

4.1 Data Modeling
4.2 OLAP Cubes
4.3 Physical Storage
4.4 Star and Snowflake Scheme
4.5 Historicization

5. Analysis Systems
   5.1 Free Data Research and OLAP
   5.2 Reporting Systems
   5.3 Model-Based Analysis Systems
   5.4 Concept-Oriented Systems

6. Distribution and Access
   6.1 Information Distribution
   6.2 Information Access

Literature

Compulsory Reading

Further Reading

- Grossmann, W., & Rinderle-Ma, S. (2015). Fundamentals of business intelligence. Springer.
- Sharda, R., Delen, D., & Turban, E. (2015). Business intelligence and analytics: Systems for decision support (10th ed.). Pearson.
- Sherman, R. (2014). Business intelligence guidebook: From data integration to analytics. Morgan Kaufmann.
- Vaisman, A., & Zimányi, E. (2022). Data warehouse systems: Design and implementation. Springer.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Business Intelligence

Course Code: DLBCSEBI02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using well-known methods and techniques from the field of Business Intelligence, students will work independently on a practical question in this course.At the end of the course you will be able to independently design and prototype Business Intelligence applications based on concrete requirements.

Course Outcomes

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Contents

- Implementation and documentation of practical questions regarding the use of Business Intelligence applications. Typical scenarios are, for example, “Management of BI projects”, “Design of multidimensional data models” and “Prototypical implementation of small BI applications”.

Literature

Compulsory Reading

Further Reading

- Liedtka, J. (2018). Why design thinking works. Harvard Business Review, 2018(9), 72–79.
- Meinel, C., & Leifer, L. J. (2021). Design thinking research: Interrogating the doing. Springer International Publishing.
- Meinel, C., Plattner, H., & Leifer, L. (2011). Design thinking: Understand – Improve – Apply. Springer Berlin Heidelberg.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Future Threats

Module Code: DLBCSEEFT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Jetzabel Maritza Serna Olvera (Threat Modeling) / N.N. (Project: Threat Modeling)

Contributing Courses to Module

- Threat Modeling (DLBCSEEFT01_E)
- Project: Threat Modeling (DLBCSEEFT02_E)

Module Exam Type

Module Exam	Split Exam
	Threat Modeling • Study Format "Distance Learning": Exam, 90 Minutes Project: Threat Modeling • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Threat Modeling

- Thinking C.I.A. and beyond
- Measuring the Cyber Threat
- Threat Modeling
- Attack libraries
- Rules, Regulations, and Law Enforcement
- Risk management
- Threat Mitigation

Project: Threat Modeling

This course covers the theory and practice of discovering and modeling threats in a given system, architecture or scenario. It covers common methodologies and sources for common threat patterns. In a project, the theory is translated to practice by analyzing a given situation for threats.

Learning Outcomes

Threat Modeling

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Project: Threat Modeling

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Threat Modeling

Course Code: DLBCSEEFT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01

Course Description

When a system or architecture is being created it is vital that possible threats are evaluated at the same time. By using both modeling methodologies and past observed attack patterns, it is possible to take a new or existing system and examine it for possible threats. With this analysis, possible risks and mitigations can be derived. While the most common methodologies are based on Attack Trees and the STRIDE model, recently attack modelling has also been using repositories of attacker techniques, tactics and procedures for inspiration.

Course Outcomes

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Contents

1. Thinking C.I.A. and beyond
    - 1.1 Confidentiality
    - 1.2 Integrity
    - 1.3 Availability
    - 1.4 Well-Known IT Security Issues
2. Measuring the Cyber Threat
    - 2.1 Concept of Threat Measuring
    - 2.2 Cyber Threat Metrics
    - 2.3 Measuring the Threat for an Organization
    - 2.4 Major Cyberattacks and their Impact
    - 2.5 Black Swan Events
3. Threat Modeling
    - 3.1 Attack Tree Methodology

Literature
Compulsory Reading
Further Reading ▪ CAPEC: Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/ ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Mitre ATT&CK®. https://attack.mitre.org/ ▪ Pfleeger, C. P. / Pfleeger, S. L. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education. ▪ Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Threat Modeling

Course Code: DLBCSEEFT02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01, DLBCSEEFT01_E or DLBCSEEFT01_D

Course Description

Threats to modern computer systems are diverse and ever evolving. In this project, the student will have the opportunity to apply the art and science of threat modeling to a scenario to be defined by the instructor together with the student. The basis will be case studies, real or fictive, to which the student will be expected to identify and report on the threats using an appropriate methodology. This can be selected from methodologies such as Attack Trees, STRIDE, DREAD or a justified enumeration of CAPEC or Mitre ATT&CK® TTPs as the student feels most appropriate. The results will be presented as a report.

Course Outcomes

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Contents

- To a given case or scenario, the student will model the threats using one of the established methodologies and then submit the report and, if appropriate, any code and data. Specific problems and contexts will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Case Studies (Cyber): https://www.securitymagazine.com/topics/2664-case-studies-cyber
- Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS.
- Palmer, C. C. (2001): Ethical Hacking. In: IBM Systems Journal. 40 (3):769.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.
- Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (Security Controls in the Cloud) / Mohammad Reza Rostami (Project: Security by Design in the Cloud)

Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECS01_E)
- Project: Security by Design in the Cloud (DLBCSEECS02_E)

Module Exam Type

Module Exam	Split Exam
	Security Controls in the Cloud • Study Format "Duales myStudium": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Security Controls in the Cloud

- Cloud security
- Losing the intranet
- Security by design
- Secure cloud coding
- Confidentiality aspects
- Monitoring and Audit

Project: Security by Design in the Cloud

This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Learning Outcomes

Security Controls in the Cloud

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Project: Security by Design in the Cloud

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Security Controls in the Cloud

Course Code: DLBCSEECS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Contents

1. Cloud security is different
    - 1.1 Shared responsibility model
    - 1.2 Infrastructure as code
    - 1.3 The Private, Public and Hybrid Cloud
    - 1.4 Types of virtualization
    - 1.5 Cloud threat models: Mitre Cloud ATT&CK
2. Losing the intranet
    - 2.1 Identify and Access Management
    - 2.2 Principle of least privilege and fine-grained cloud access control
    - 2.3 Using Software Defined Networks, virtual private clouds and subnets
    - 2.4 Moving to a serverless architecture
    - 2.5 Defense in depth

3. Security by design
   - 3.1 Orchestration: Infrastructure as Code
   - 3.2 The Automate-Everything principle, Updating and Repeatability
   - 3.3 Reuse of good design patterns
   - 3.4 Container security
   - 3.5 Identification and Authentication

4. Secure cloud coding
   - 4.1 Software supply chain security
   - 4.2 Continuous Integration and Deployment
   - 4.3 Testing in code integration for security
   - 4.4 Canaries in code deployment
   - 4.5 Policy engines

5. Confidentiality aspects
   - 5.1 Secrets management
   - 5.2 Encryption of data at rest
   - 5.3 Encryption of data in transit
   - 5.4 Data leakage and exfiltration

6. Availability
   - 6.1 Storage tiers and locality
   - 6.2 Backup strategies
   - 6.3 Data and process redundancy
   - 6.4 Data lifecycle configuration
   - 6.5 DDoS mitigation

7. Locality
   - 7.1 Compliance requirements
   - 7.2 Geography of data/processes
   - 7.3 Redundancy of data centers
   - 7.4 Colocation for performance reasons

8. Monitoring and Audit
   - 8.1 Centralized logging
   - 8.2 Auditing orchestration scripts
   - 8.3 Detecting misconfigurations
   - 8.4 Cloud Forensics

9. Summary and Research topics
   - 9.1 Homomorphic encryption
   - 9.2 Attestation
   - 9.3 Proof-carrying data
   - 9.4 Side-channel attacks
   - 9.5 Conclusions

Literature
Compulsory Reading
Further Reading ▪ Mitre Cloud ATT&CK. https://attack.mitre.org/matrices/enterprise/cloud/

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E

Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Literature

Compulsory Reading

Further Reading

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Vulnerability Analysis and Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Enno Nagel (Principles of Ethical Hacking) / Prof. Dr. Björn Kaidel (Project: Pentesting)

Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEEPT01_E)
- Project: Pentesting (DLBCSEEPT02_E)

Module Exam Type

Module Exam	Split Exam
	Principles of Ethical Hacking • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes Project: Pentesting • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Principles of Ethical Hacking

- Introduction to Ethical Hacking
- Reconnaissance
- Enumeration and Vulnerability Analysis
- Hacking Systems
- Malware

Project: Pentesting

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.

Learning Outcomes

Principles of Ethical Hacking

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Project: Pentesting

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Contents

1. Introduction to Ethical Hacking
    - 1.1 Overview of Cyber Security
    - 1.2 Concepts of Cyber Kill Chain
    - 1.3 Hacking vs Ethical Hacking
    - 1.4 Laws and Standards
2. Reconnaissance
    - 2.1 Footprinting Techniques
    - 2.2 Network Scanning
    - 2.3 Host Discovery
    - 2.4 Service, Port and OS Discovery
    - 2.5 Scan beyond Security Measures
3. Enumeration and Vulnerability Analysis
    - 3.1 Enumeration Techniques
    - 3.2 Enumeration Countermeasures
    - 3.3 Vulnerability Assessment Techniques

- 3.4 Vulnerability Classification and Assessment

4. Hacking Systems
   - 4.1 Gaining Access to Systems
   - 4.2 Privilege Escalation
   - 4.3 Persistent Access
   - 4.4 Covering Traces

5. Malware
   - 5.1 Types of Malware
   - 5.2 Concepts of Fileless Malware
   - 5.3 Countermeasures

6. Sniffing
   - 6.1 Concepts of Sniffing
   - 6.2 Sniffing Techniques
   - 6.3 Countermeasures

7. Denial of Service
   - 7.1 Concepts of DoS/DDoS
   - 7.2 Attack Techniques
   - 7.3 Botnets
   - 7.4 Countermeasures

8. Social Engineering
   - 8.1 Concepts of Social Engineering
   - 8.2 Social Engineering Techniques
   - 8.3 Identity Theft and Impersonation
   - 8.4 Countermeasures

Literature
Compulsory Reading
Further Reading ▪ Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]). ▪ Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/ ▪ Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/ ▪ Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/ ▪ Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769. ▪ Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Pentesting

Course Code: DLBCSEEPT02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E

Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Industrial Systems Technology

Module Code: DLBCSEEIST_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Markus Kleffmann (Software Engineering Principles) / Dr. Rachel John Robinson (Internet of Things Security)

Contributing Courses to Module

- Software Engineering Principles (IGIS01_E)
- Internet of Things Security (DLBCSEEIST01_E)

Module Exam Type

Module Exam	Split Exam
	Software Engineering Principles • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Internet of Things Security • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Software Engineering Principles

- binary system
- Structure and function of computer systems
- Structure and function of communication networks
- Software life cycle
- Roles, phases, activities in software engineering

Internet of Things Security

Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Learning Outcomes

Software Engineering Principles

On successful completion, students will be able to

- perform simple calculations in the binary system (Boolean algebra).
- describe the structure of computer systems and communication networks.
- distinguish between the phases of a SW life cycle.
- distinguish roles and phases in the software process.
- know different process models of SW development.
- know typical challenges and risks of enterprise SW development.
- know different programming paradigms and their application.

Internet of Things Security

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Software Engineering Principles

Course Code: IGIS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of the course is to give students an insight into the technical and theoretical basics of software engineering. In addition to the general structure of computer systems, students are taught typical challenges in the development of enterprise information systems. Furthermore, the typical phases and activities in software engineering are presented to address these risks.

Course Outcomes

On successful completion, students will be able to

- perform simple calculations in the binary system (Boolean algebra).
- describe the structure of computer systems and communication networks.
- distinguish between the phases of a SW life cycle.
- distinguish roles and phases in the software process.
- know different process models of SW development.
- know typical challenges and risks of enterprise SW development.
- know different programming paradigms and their application.

Contents

1. Structure and organization of information systems
   - 1.1 0 and 1 as the basis of all IT systems
   - 1.2 Von Neumann Architecture
   - 1.3 Distributed systems and communication networks
   - 1.4 Enterprise information systems

2. Risks and challenges of enterprise software engineering
   - 2.1 Properties of enterprise software systems
   - 2.2 Software Engineering
   - 2.3 Risks and typical problems
   - 2.4 Root cause analysis
   - 2.5 Challenges in Software Engineering

3. Software life cycle: from planning to replacement
   - 3.1 The software life cycle at a glance

- 3.2 Planning
- 3.3 Development
- 3.4 Operation
- 3.5 Maintenance
- 3.6 Shutdown

4. Requirements engineering and specification
   - 4.1 requirements engineering
   - 4.2 Specification

5. Architecture and implementation
   - 5.1 Architecture
   - 5.2 Implementation

6. Testing, operation and evolution
   - 6.1 Testing
   - 6.2 Operation
   - 6.3 Evolution

7. Roles in Software Engineering
   - 7.1 Idea of the role-based approach
   - 7.2 Typical roles

8. Organization of software projects
   - 8.1 From process paradigm towards software process
   - 8.2 Process Paradigms

9. Software Process Frameworks
   - 9.1 V-model XT
   - 9.2 Rational Unified Process (RUP)
   - 9.3 Scrum

Literature
Compulsory Reading
Further Reading ▪ Pohl, K., & Rupp., C. (2015). Requirements engineering (2nd ed.). Rocky Nook. ▪ Sommerville, I. (2016). Software engineering (10th ed.). Pearson. ▪ Sommerville, I. (2019). Engineering software products: An introduction to modern software engineering. Pearson. ▪ Jacobson, I., Lawson, H., & Ng, P.-W. (2019). The essentials of modern software engineering. ACM Books.

Study Format myStudies

Study Format	**Course Type**
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Internet of Things Security

Course Code: DLBCSEEIST01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBINGEIT01_E or DLBINGEIT01

Course Description

Internet of Things (IoT) is a mega trend. It covers end consumer systems as well as industrial systems and technologies (Industrial IoT, or IIoT). There is an increasing amount of interconnected devices that composes the Internet of Things. In general, the Internet of Things architecture consists of terminal devices, cloud solutions and actors/sensors. Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Course Outcomes

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Contents

1. Basics of the Internet of Things (IoT)
   - 1.1 Introduction
   - 1.2 Architecture
   - 1.3 Non-Industrial Internet of Things
   - 1.4 Industry 4.0 (Industrial IoT)
2. Internet of Things Attacks
   - 2.1 Vulnerabilities, Threats and Risks
   - 2.2 Cyber Attacks and Countermeasures
3. Security by Design
   - 3.1 Project Management / Secure Development Life Cycle
   - 3.2 Static Testing
   - 3.3 Dynamic Testing
   - 3.4 DevSecOps

4. Securing Internet of Things Devices
   - 4.1 Security Risks
   - 4.2 Design Objectives

5. Operational Security
   - 5.1 Information and Cyber Security Management System
   - 5.2 Network Security
   - 5.3 Device Configuration
   - 5.4 Authentication and Authorization

6. Cloud Security
   - 6.1 Concept of the Fog
   - 6.2 Threats to Cloud Internet of Things Services
   - 6.3 Cloud-Based Security Services
   - 6.4 Securing the Cloud Solution

7. Big Data / Artificial Intelligence
   - 7.1 Supervised Learning
   - 7.2 Unsupervised Learning

Literature

Compulsory Reading

Further Reading

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum		WiSe/SoSe	English

Module Coordinator

Dr. Christian Prause (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01_E)
- Project: Defense against APTs (DLBCSEECTI02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Threat Feeds • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Project: Defense against APTs • Study Format "myStudies": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Attack Models and Threat Feeds

- Threat actors
- Modeling an Attack
- Attack Preparation TTPs
- Enterprise TTPs
- Industrial Control Systems TTPs
- Reporting

Project: Defense against APTs

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a "table top exercise" which data is already available and which extern threat feed data is required. After analyzing the "attack side" students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

Learning Outcomes

Attack Models and Threat Feeds

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Project: Defense against APTs

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a "table top exercise".
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Attack Models and Threat Feeds

Course Code: DLBCSEECTI01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data.It is rare that internal data is enough for a complete analysis and in practice the threat analysist must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience.After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Contents

1. Threat Actors
    - 1.1 Script Kiddies
    - 1.2 eCrime Threat Actors
    - 1.3 Advanced Persistent Threat Actors (APT)
    - 1.4 Threat Researchers
2. Modeling an Attack
    - 2.1 Phases of an Attack
    - 2.2 Lockheed Martin Kill-Chain
    - 2.3 Attack Trees
    - 2.4 Models for Security Risks and Cyber Attacks

3. Attack preparation TTPs
   - 3.1 Observability of Attack Preparations
   - 3.2 Operational Security of an Organization

4. Enterprise TTPs
   - 4.1 Behaviors of the Attacker
   - 4.2 Observable Data in an Enterprise

5. Industrial Control Systems TTPs
   - 5.1 Critical Infrastructure
   - 5.2 Special Considerations with IoT/ICS Defense

6. Threat data exchange
   - 6.1 Indicators of Compromise vs. Indicators of Attack
   - 6.2 Threat Intelligence Reports
   - 6.3 Ad-hoc Data Formats
   - 6.4 STIX Format, TAXII Protocol
   - 6.5 Semantics of Threat Data using Mitre ATT&CK, CVEs, etc.

7. Examples of Threat Analysis Platforms
   - 7.1 ACT Platform
   - 7.2 MISP
   - 7.3 OpenCTI

8. Examples of Threat Actors and their Modus Operandi
   - 8.1 Threat Model
   - 8.2 Relevant Indicator Data
   - 8.3 Relevant CTI Data
   - 8.4 Diagnosing the Threat
   - 8.5 Data Coverage Gap Analysis

9. Reporting
   - 9.1 Mapping Raw Data to Mitre ATT&CK
   - 9.2 Making Defensive Recommendations
   - 9.3 Writing Reports for Technical Staff
   - 9.4 Writing Reports for Management
   - 9.5 Working with Law Enforcement

Literature
Compulsory Reading
Further Reading ▪ Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. Retrieved from http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf ▪ Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2010). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved from https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LMWhite-Paper-Intel-Driven-Defense.pdf ▪ MISP Project. (n.d.). Retrieved from https://www.misp-project.org/ ▪ Mitre ATT&CK. (n.d.). Retrieved from https://attack.mitre.org/ ▪ Obrst, L., Chase, P., & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security. Fairfax, VA.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Defense against APTs

Course Code: DLBCSEECTI02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT´s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures.
To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT´s, ISP´s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a

comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT´s, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Mobile Threats

Module Code: DLBCSEEMT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Mohammad Reza Rostami (Wireless and Telecom Security) / Prof. Dr. Jörn-Marc Schmidt (Software Architectures of Mobile Devices)

Contributing Courses to Module

- Wireless and Telecom Security (DLBCSEEMT01_E)
- Software Architectures of Mobile Devices (DLBCSEEMT02_E)

Module Exam Type

Module Exam	Split Exam
	Wireless and Telecom Security • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes Software Architectures of Mobile Devices • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module
see curriculum

Module Contents

Wireless and Telecom Security

- Wireless protocols overview
- Wireless basics
- Telecom protocol classes
- Telecom architecture
- Handset and device security
- Threats
- Other wireless applications
- Protections

Software Architectures of Mobile Devices

- Handset technology stack
- Hardware
- Android operating system
- Apple iOS operating system
- Mobile devices
- Software ecosystems and security
- Mobile handset threats
- Mobile Device Management

Learning Outcomes

Wireless and Telecom Security

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Software Architectures of Mobile Devices

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Wireless and Telecom Security

Course Code: DLBCSEEMT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBIBRVS01_E or DLBIBRVS01; DLBCSEINF01_E or DLBCSEINF01_D

Course Description

The number of devices that can connect wirelessly to networks has already overtaken the number of desktop and laptop computers that connect to a local area network via a cable. In particular, phones and tablets dominate the market, and these connect to the wireless telecommunication networks. But there are also many other forms of wireless communication that devices use. The idiosyncrasies of these wireless systems need to be understood to integrate them in a complete security concept. Wireless protocols often force the user to trust in a system that they have no insights into and in this course, we will shine light onto the subject.

Course Outcomes

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Contents

1. Wireless protocols overview
    - 1.1 Personal area network protocols (Bluetooth, RFID, NFC, and more)
    - 1.2 Wireless local area network protocols (802.11a,b, g, ac , p and more)
    - 1.3 Wide area network protocols (Telecom protocols, LoRa, Satellite protocols, and more)
    - 1.4 Key exchange and cryptography in wireless networking
2. Wireless basics
    - 2.1 Frequencies
    - 2.2 Modulations
    - 2.3 Data Encodings
    - 2.4 Trade-offs
3. Telecom protocol classes

- 3.1 Telecom vs IT terminology and technologies
- 3.2 Telecom standards
- 3.3 Legacy digital protocols
- 3.4 LTE
- 3.5 5G

4. Telecom architecture
   - 4.1 Overall architecture
   - 4.2 Core architecture
   - 4.3 Software defined networking
   - 4.4 5G Campus Networks
   - 4.5 Application layer security

5. Handset and device security
   - 5.1 Requirements
   - 5.2 Typical hardware design
   - 5.3 IoT Devices

6. Threats
   - 6.1 Common attack vectors against devices and handsets
   - 6.2 Common attack vector against the core network
   - 6.3 Potential attacks against 5G campus networks

7. Other wireless applications
   - 7.1 Aviation and Nautical wireless protocols
   - 7.2 Proprietary device protocols
   - 7.3 Wide area sensor networks (LoRa, Sigfox, ...)
   - 7.4 Digital voice/data technologies (DECT/GAP, TETRA, ...)
   - 7.5 Satellite communications

8. Protections
   - 8.1 Integrating mobile technology securely
   - 8.2 Monitoring mobile devices

Literature
Compulsory Reading
Further Reading ▪ Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G. ▪ Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187. ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Software Architectures of Mobile Devices

Course Code: DLBCSEEMT02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Mobile devices have supplanted desktops and laptops as the most common end-user device. The smart phone has become a central business tool. Users run their entire lives from them. Furthermore, the Internet of Things are also using these mobile platforms. But too often, the risks and opportunities associated with these mobile devices are opaque to the security administrators in particular as these devices often operate outside the traditional Intranet. In this course, we examine how the dominant players, Android and Apple iOS, handle security in their software stack and ecosystem. We also look at the overlooked problem of IoT Security and wrap up with organizational solutions.

Course Outcomes

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Contents

1. Handset technology stack
    - 1.1 Hardware
    - 1.2 Firmware
    - 1.3 Operating system
    - 1.4 Applications
    - 1.5 Ecosystem
2. Hardware
    - 2.1 RF modules
    - 2.2 PDA module
    - 2.3 Trusted Execution Environment component
    - 2.4 Biometric devices
    - 2.5 Location technology

3. Android operating system
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel and Hardware abstraction layer
   - 3.4 Sandboxing and virtualization
   - 3.5 Code signing

4. Apple iOS operating system
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel and Frameworks
   - 4.4 Sandboxing and virtualization
   - 4.5 Code signing

5. Mobile devices
   - 5.1 The Internet of things
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android on devices
   - 5.5 Other common embedded operating systems

6. Software ecosystems and security
   - 6.1 Google play
   - 6.2 Apple store
   - 6.3 Security providers
   - 6.4 The role of the Cloud

7. Mobile handset threats
   - 7.1 Historic examples of handset attacks
   - 7.2 Taxonomy of Handset threats
   - 7.3 Jailbreaking

8. Mobile Device Management
   - 8.1 The threats of BYOD
   - 8.2 Unique threats to mobile devices
   - 8.3 Patch and policy management

Literature
Compulsory Reading
Further Reading ▪ Gupta, A. (2014): Learning Pentesting for Android Devices ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ N.A. (2020): Android Enterprise Security White Paper. ▪ N.A. (2019): iOS Security iOS 12.3. https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf ▪ Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Supply Chain Management

Module Code: DLBDSESCM

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alex Leberling (Supply Chain Management I) / N.N. (Supply Chain Management II)

Contributing Courses to Module

- Supply Chain Management I (DLBDSESCM01)
- Supply Chain Management II (DLBDSESCM02)

Module Exam Type

Module Exam	Split Exam
	Supply Chain Management I • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Supply Chain Management II • Study Format "myStudies": Exam or Advanced Workbook, 90 Minutes • Study Format "Distance Learning": Exam or Advanced Workbook, 90 Minutes

Weight of Module

see curriculum

Module Contents

Supply Chain Management I

- Historical and terminological aspects of the SCM concept
- Motives for the creation of cross-company value creation networks
- Design principles and effects of value creation networks
- Logistical core processes and SCM
- Information technology aspects of the SCM concept
- Coordination and collaboration of the network partners
- Industry-specific solutions of the SCM

Supply Chain Management II

- Strategic aspects of SCM
- SCM Practice: Tasks and Activities in the Core Planning Process
- SCM Practice: Tasks and Activities in the Core Process of Procurement
- SCM Practice: Tasks and Activities in the Core Process Production
- SCM Practice: Tasks and Activities in the Core Distribution Process

Learning Outcomes

Supply Chain Management I

On successful completion, students will be able to

- explain the importance of cross-company value creation processes.
- understand common concepts for modeling cross-company value creation processes.
- understand dynamic effects in supply chains and can systematize their causes and effects.
- explain important theoretical concepts for describing the characteristics and challenges of cross-company value creation processes.
- explain the approaches and problem categories commonly used in the context of supply chain management.
- understand important reference and/or management models for the concretization of supply chain systems.
- name and detail important roles and tasks in the SCM network.
- deal with the coordination problem of SCM and describe the common solution approaches.

Supply Chain Management II

On successful completion, students will be able to

- systematically explain the strategic relevance of enterprise-wide value creation processes.
- understand the most important tasks and problems in the SCM core process planning.
- systematize the elements and interrelationships in the CPFR model in a differentiated way.
- be familiar with the characteristics and peculiarities of contract logistics.
- understand the most important tasks and problems in the SCM core process procurement.
- explain central elements and characteristics of a procurement strategy.
- understand the most important tasks and problems in the SCM core process production.
- explain central elements and characteristics of a modern production strategy.
- understand the most important tasks and problems in the SCM core process distribution.
- explain central elements and characteristics of the so-called ECR concept.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Logistics & Transportation	All Bachelor Programmes in the Transport & Logistics fields

Supply Chain Management I

Course Code: DLBDSESCM01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

SCM proves to be an extremely multi-faceted construct from both a theoretical and a practical point of view. An adequate understanding of the problem dimensions and modes of action of (global) cross-company value creation networks requires a multidimensional approach. It starts by considering logistical processes, with modern process, flow, and network standards forming an important basis for SCM. On the basis of such an approach, students should gain a fundamental understanding of SCM. From the point of view of a holistic approach, it also makes sense to also examine a number of other typical problem areas in addition to the logistical challenges of this concept. This includes IT aspects of SCM (e.g., APS systems), and questions to do with the collaboration and coordination of network partners. This course also considers selected industry specific SCM solutions (ECR or VMI).

Course Outcomes

On successful completion, students will be able to

- explain the importance of cross-company value creation processes.
- understand common concepts for modeling cross-company value creation processes.
- understand dynamic effects in supply chains and can systematize their causes and effects.
- explain important theoretical concepts for describing the characteristics and challenges of cross-company value creation processes.
- explain the approaches and problem categories commonly used in the context of supply chain management.
- understand important reference and/or management models for the concretization of supply chain systems.
- name and detail important roles and tasks in the SCM network.
- deal with the coordination problem of SCM and describe the common solution approaches.

Contents

1. Fundamentals of the Supply Chain Concept
    - 1.1 Terminological and Conceptual Fundamentals
    - 1.2 Supply Chain Typology According to Otto
    - 1.3 Supply Chain Typology According to Bechtel/Jayaram
    - 1.4 Dynamic Aspects of Supply Chains

2. Selected Theoretical Concepts for the Supply Chain Concept
   - 2.1 New Institutional Economics
   - 2.2 Game Theory
   - 2.3 Network Approach
   - 2.4 Other Theoretical Additions

3. Supply Chain Management
   - 3.1 Basic Information on the Goals and Scope of SCM
   - 3.2 Popular Problem Areas of the SCM
   - 3.3 Supply Chain Management as an Evolutionary Step in Logistics
   - 3.4 Supply Chain Management as Cooperation Management

4. SCM Model
   - 4.1 Basic Information on the Term SCM Models
   - 4.2 SCOR Model
   - 4.3 SCM Task Model

5. SCM as a Coordination Problem
   - 5.1 Basic Information on the Concept of Coordination
   - 5.2 Coordination Concepts, Context, and Perspectives of SCM
   - 5.3 Coordination Instruments

Literature

Compulsory Reading

Further Reading

- Bowersox, J., Closs, D., & Cooper, M. B. (2020). Supply chain logistics management (5th ed.). McGraw Hill Education.
- Chopra, S., & Meindl, P. (2019). Supply chain management: Strategy, planning, and operation (7th ed., Global ed.). Pearson Education.
- Es-Satty, Asmaa; Lemghari, Radouane; Okar, Chafik. (2020). Supply Chain Digitalization Overview SCOR model implication. In: 2020 IEEE 13th International Colloquium of Logistics and Supply Chain Management (LOGISTIQUA) Logistics and Supply Chain Management (LOGISTIQUA), 2020 IEEE 13th International Colloquium of. :1-7 Dec, 2020; IEEE Language: English, Datenbank: IEEE Xplore Digital Library.
- Tarigan, Z. J. H., Siagian, H., & Jie, F. (2021). Impact of enhanced enterprise resource planning (ERP) on firm performance through green supply chain management. Sustainability, 13(8), article 4358.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Supply Chain Management II

Course Code: DLBDSESCM02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

From the perspective of strategic management research and practice, the activities covered by the term SCM are closely related to efforts to build and/or maintain a stable operational competitive advantage. A fundamental discussion of this relationship forms the starting point for the course. On this basis, a differentiated analysis of strategy-relevant activities and instruments in the Plan, Source, Make, Deliver, and Return process categories is then carried out using the SCOR model. Special attention is given to the practice-relevant areas of SCM, e.g., order-promising (plan), supplier-relation-management (source), postponement (make), and the ECR-concept (deliver).

Course Outcomes

On successful completion, students will be able to

- systematically explain the strategic relevance of enterprise-wide value creation processes.
- understand the most important tasks and problems in the SCM core process planning.
- systematize the elements and interrelationships in the CPFR model in a differentiated way.
- be familiar with the characteristics and peculiarities of contract logistics.
- understand the most important tasks and problems in the SCM core process procurement.
- explain central elements and characteristics of a procurement strategy.
- understand the most important tasks and problems in the SCM core process production.
- explain central elements and characteristics of a modern production strategy.
- understand the most important tasks and problems in the SCM core process distribution.
- explain central elements and characteristics of the so-called ECR concept.

Contents

1. Strategic Aspects of SCM
   - 1.1 Strategic Thinking and Action: General Information
   - 1.2 Competition Focus and SCM
   - 1.3 Competition Location and SCM
   - 1.4 Competition Rules and SCM

2. SCM Practice: Core Process Planning
   - 2.1 General Preliminary Considerations
   - 2.2 Collaborative Planning, Forecasting, and Replenishment
   - 2.3 Order Promoting

2.4 Kanban
2.5 Integration of X-PL Logistics Service Providers

3. SCM Practice: Core Process Procurement
   3.1 General Preliminary Considerations
   3.2 Production Synchronous Procurement
   3.3 Sourcing Concepts
   3.4 Supplier Relations Management

4. SCM Practice: Core Process Production
   4.1 Selected Aspects of the Problem Background
   4.2 Collaborative Engineering
   4.3 Postponement Strategies
   4.4 Value Added Partnership

5. SCM Practice: Core Process Distribution
   5.1 Basic Information on the Distribution Problem
   5.2 Efficient Consumer Response (ECR)
   5.3 Consignment Warehouse

Literature

Compulsory Reading

Further Reading

- Chopra, S. (2019). Supply chain management: Strategy, planning and operation (Global ed., 7th ed.). Pearson.
- Hill, A., & Hill, T. (2018). Essential operations management (2nd ed.). Palgrave.
- Hugos, M. (2011). Essentials of supply chain management (3rd ed.). John Wiley & Sons.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam or Advanced Workbook, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
100 h	0 h	25 h	25 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam or Advanced Workbook, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
100 h	0 h	25 h	25 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Smart Factory

Module Code: DLBDSESF

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Sahar Qaadan (Smart Factory) / Dr. Sahar Qaadan (Project: Smart Factory)

Contributing Courses to Module

- Smart Factory (DLBDSESF01)
- Project: Smart Factory (DLBDSESF02)

Module Exam Type

Module Exam	Split Exam
	Smart Factory • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Smart Factory • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Smart Factory

- Motivation and Definition of Terms
- Development of Automation
- Technological Basics and Standards
- Basic concepts of a Smart Factory
- Reference Architectures
- Smart Factory Engineering
- Safety and Security

Project: Smart Factory

A catalogue with the currently provided tasks is provided on the online platform of the module. It provides the content basis of the module and can be supplemented or updated by the seminar leader.

Learning Outcomes

Smart Factory

On successful completion, students will be able to

- understand the term Smart Factory in the context of Industry 4.0.
- be able to trace the development of automation to a fully autonomous, non-centrally organized production plant.
- understand the basic technologies and standards used to design and operate a Smart Factory.
- understand the essential concepts of a Smart Factory.
- identify and differentiate between the individual elements of a Smart Factory using different reference architectures.
- understand the special engineering challenges in the Smart Energy context.
- understand the special safety risks of digitized and networked production plants and assign concrete recommendations for action.

Project: Smart Factory

On successful completion, students will be able to

- have a deeper understanding of the technologies and standards in the context of Smart Factory.
- apply technologies in the context of Smart Factory to a simple practical example.
- design a hardware or software prototype for a selected task.
- document, design, and develop activities in the form of a project report.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology field

Smart Factory

Course Code: DLBDSESF01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students will gain a deeper insight into the networking and digitization of production facilities by examining a Smart Factory. For this purpose, they will be familiarized with the basic goals of a Smart Factory in the context of the research complex Industry 4.0. After a brief introduction to the history of automation, students will learn the technical basics and standards required to design and operate a Smart Factory. Building on this, they will learn how these individual technologies are used to implement the central concepts of a Smart Factory. In order to understand which components a Smart Factory consists of, different reference architectures are presented and compared. The course concludes with the special engineering challenges of an autonomously acting and decentralized production plant. Above all, this includes IT security, which is particularly relevant due to the digital networking of production facilities and products.

Course Outcomes

On successful completion, students will be able to

- understand the term Smart Factory in the context of Industry 4.0.
- be able to trace the development of automation to a fully autonomous, non-centrally organized production plant.
- understand the basic technologies and standards used to design and operate a Smart Factory.
- understand the essential concepts of a Smart Factory.
- identify and differentiate between the individual elements of a Smart Factory using different reference architectures.
- understand the special engineering challenges in the Smart Energy context.
- understand the special safety risks of digitized and networked production plants and assign concrete recommendations for action.

Contents

1. Motivation and Definition of Terms
    - 1.1 Goals of Smart Factory
    - 1.2 Internet of Things
    - 1.3 Cyber-Physical Systems
    - 1.4 Cyber-Physical Production Systems
    - 1.5 Smart Factory as a Cyber-Physical (Production) System

2. Development of Automation
   - 2.1 Automation Pyramid
   - 2.2 Networked, Decentralized Organization of Production
   - 2.3 Future Challenges

3. Technological Basics and Standards
   - 3.1 Identification of Physical Objects
   - 3.2 Formal Description Languages and Ontologies
   - 3.3 Digital Object Memory
   - 3.4 Physical Situation Recognition
   - 3.5 (Partially) Autonomous Action and Cooperation
   - 3.6 Human-Machine Interaction
   - 3.7 Machine to Machine Communication

4. Basic Concepts of a Smart Factory
   - 4.1 Order-Controlled Production
   - 4.2 Bundling of Machine and Production Data
   - 4.3 Supporting People in Production
   - 4.4 Intelligent Products and Resources
   - 4.5 Smart Services

5. Reference Architectures
   - 5.1 Purpose and Properties of Reference Architectures
   - 5.2 Overview of Standardization Initiatives
   - 5.3 CyProS Reference Architecture
   - 5.4 RAMI 4.0 (DIN SPEC 91345)

6. Smart Factory Engineering
   - 6.1 Classification of Different Engineering Tools
   - 6.2 Virtual Engineering
   - 6.3 User-Centered Design
   - 6.4 Requirements Engineering
   - 6.5 Modelling
   - 6.6 Integration of Classic and Smart Components

Literature
Compulsory Reading
Further Reading ▪ Butun, I. (2020). Industrial IoT: Challenges, design principles, applications, and security. Springer. ▪ Drossel, W. G., Ihlenfeldt, S., Lanzger, T., & Dumitrescu, R. (2019). Cyber-physical systems. In R. Neugebauer (Ed.), Digital transformation (pp. 189—213). Springer. ▪ Durakbasa, N. M., & Gençyılmaz, M. G. (Eds.). (2021). Digital conversion on the way to Industry 4.0. Springer. ▪ Ustundag, A., & Cevikcan, E. (2018). Industry 4.0: Managing the digital transformation. Springer.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Slides	

Project: Smart Factory

Course Code: DLBDSESF02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students select a concrete task from the catalog of topics provided in consultation with the seminar leader. They will work on the task in a prototyping environment suited to the task, which can be either a hardware (e.g., prototyping boards) or software (e.g., technology-specific development environments) environment. To complete the task, students apply the concepts, methods, and tools taught in the Smart Factory I course. They document their results with a project report.

Course Outcomes

On successful completion, students will be able to

- have a deeper understanding of the technologies and standards in the context of Smart Factory.
- apply technologies in the context of Smart Factory to a simple practical example.
- design a hardware or software prototype for a selected task.
- document, design, and develop activities in the form of a project report.

Contents

- A catalogue with the currently provided tasks is provided on the online platform of the module. It provides the content basis of the module and can be supplemented or updated by the seminar leader.

Literature
Compulsory Reading
Further Reading ▪ Arey, D., Le, C. H. & Gao, J. (2021). Lean industry 4.0: a digital value stream approach to process improvement. Procedia Manufacturing, 54, 19–24. ▪ Hartmann, L., Meudt, T., Seifermann, S. & Metternich, J. (2018). Value stream method 4.0: holistic method to analyse and design value streams in the digital age. Procedia CIRP, 78, 249–254. ▪ Luscinski, S. & Ivanov, V. (2020). A Simulation Study of Industry 4.0 Factories based on the Ontology on Flexibility with using FlexSim Software. Management and Production Engineering Review (volume 11, number 3), S. 74–83. ▪ Meroni, G., Baresi, L., Montali, M. & Plebani, P. (2017). Multi-party business process compliance monitoring through IoT-enabled artifacts. Information Systems, 73, 61-78. ▪ OMG (2014). Business Process Model and Notation (BPMN). Version 2.0.2

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
Tutorial Support ☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	**Exam Preparation** ☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
Tutorial Support ☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	**Exam Preparation** ☑ Guideline

Production Engineering, Automation and Robotics

Module Code: DLBDSEAR

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Hans Kerwat (Production Engineering Industry 4.0) / Ha Ngo (Automation and Robotics)

Contributing Courses to Module

- Production Engineering Industry 4.0 (DLBDSEAR01)
- Automation and Robotics (DLBDSEAR02)

Module Exam Type

Module Exam	Split Exam
	Production Engineering Industry 4.0 • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Automation and Robotics • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Production Engineering Industry 4.0

- Introduction to Manufacturing Technology
- Main Production Groups According to DIN 8580
- Additive Manufacturing Processes
- Rapid Prototyping
- Rapid Tooling
- Direct/Rapid Manufacturing
- Cyber-Physical Production Plants

Automation and Robotics

- Basics of Automation
- Fundamentals of Measurement Technology
- Sensors
- Basics of Control Engineering
- Basics of Control Technology
- Introduction to Robotics
- Kinematics of a Robot

Learning Outcomes

Production Engineering Industry 4.0

On successful completion, students will be able to

- understand the basic concepts and interrelationships of production engineering.
- understand current changes in manufacturing technology due to technologies such as additive manufacturing and megatrends such as cyber physical systems.
- assign different manufacturing processes to the main manufacturing groups according to DIN 8580.
- understand the basic principle of additive manufacturing processes.
- distinguish between different additive manufacturing processes.
- understand the terms Rapid Prototyping, Rapid Tooling, and Direct Manufacturing and name individual processes and application examples.
- understand the elements and properties of cyber-physical production plants.

Automation and Robotics

On successful completion, students will be able to

- understand the basic aspects of automation.
- understand the different sizes and units in measurement technology.
- differentiate between different measurement methods.
- understand the basic structure of measuring equipment.
- select a suitable sensor based on various criteria.
- understand the elements of control systems.
- describe the behavior of control systems in the time and frequency domain.
- understand the basic principles of control technology.
- convert between different number systems and apply Boolean algebra.
- understand the structure of switching networks, plants, and storages.
- understand important elements of control systems such as signal generators and power amplifiers.
- design simple programmable logic controllers.
- understand the basic structure of industrial robots.
- calculate different movements and positions of jointed-arm robots.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Engineering	All Bachelor Programmes in the IT & Technology fields

Production Engineering Industry 4.0

Course Code: DLBDSEAR01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of the course is to provide students with an overview of the processes that have influenced and still influence production processes through technological developments under the generic term Industry 4.0, based on traditional, standardized manufacturing techniques. These include, in particular, technological advances in additive manufacturing processes that enable applications such as rapid prototyping, rapid tooling, and direct manufacturing. Finally, the course deals with the consequences of the digitalization and networking of production facilities and their elements in the sense of a cyber-physical system.

Course Outcomes

On successful completion, students will be able to

- understand the basic concepts and interrelationships of production engineering.
- understand current changes in manufacturing technology due to technologies such as additive manufacturing and megatrends such as cyber physical systems.
- assign different manufacturing processes to the main manufacturing groups according to DIN 8580.
- understand the basic principle of additive manufacturing processes.
- distinguish between different additive manufacturing processes.
- understand the terms Rapid Prototyping, Rapid Tooling, and Direct Manufacturing and name individual processes and application examples.
- understand the elements and properties of cyber-physical production plants.

Contents

1. Introduction to Manufacturing Technology
    - 1.1 Basic Terms and Contexts in Manufacturing Theory
    - 1.2 Historical Development of Production
    - 1.3 The Discussion About the Long Tail
2. Classification Of Manufacturing Processes
    - 2.1 Casting and Molding
    - 2.2 Forming
    - 2.3 Machining
    - 2.4 Joining

- 2.5 Coating
- 2.6 Changing the Properties of Substances

3. Additive Manufacturing Processes
   - 3.1 Basic Principles and Legal Aspects
   - 3.2 Stereolithography (STL)
   - 3.3 Selective Laser Sintering and Selective Beam Melting With Laser or Electron Beam
   - 3.4 Fused Deposition Modeling (FDM)
   - 3.5 Multi-Jet Modeling (MJM) and Poly-Jet Process (PJM)
   - 3.6 3D Printing Process (3DP)
   - 3.7 Laminating Processes
   - 3.8 Mask Sintering

4. Rapid Prototyping
   - 4.1 Definition
   - 4.2 Strategic and Operational Aspects
   - 4.3 Application Areas and Examples

5. Rapid Tooling
   - 5.1 Definition, Strategic, and Operational Aspects
   - 5.2 Indirect and Direct Procedures

6. Direct/Rapid Manufacturing
   - 6.1 Potentials and Requirements for Procedures
   - 6.2 Implementation, Application Areas, and Examples

7. Cyber-Physical Production Plants
   - 7.1 Derivation of the Terms Industry 4.0 and Cyber-Physical Systems
   - 7.2 Megatrend Cyber Physical Systems (CPS)
   - 7.3 Definition Cyber-Physical Production Plant
   - 7.4 Effects on Planning and Operation of Production Facilities
   - 7.5 Dynamic Reconfiguration and Migration of Production Facilities

Literature
Compulsory Reading
Further Reading ▪ Anderson, C. (2012). Makers: The new industrial revolution. Crown Business. ▪ Gebhardt, A., Kessler, J. & Thurn, L. (2019). 3D printing: Understanding additive manufacturing (2nd ed). Hanser. ▪ Groover, M. P. (2012). Fundamentals of modern manufacturing: Materials, processes, and systems (5th ed.). Wiley.

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Automation and Robotics

Course Code: DLBDSEAR02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of the course is to provide students with an insight into measurement, control, and regulation technology and convey the basics of robotics. Students will be taught which methods can be used to determine certain measured variables and how measurement errors are dealt with. Based on these fundamentals, various sensors will be presented and students will be able to select suitable sensors based on predefined criteria. The course also introduces students to the basics of control engineering. The different ways of describing the structure and behaviour of control systems are illustrated to the students. The basics of control engineering are also taught. The students receive a short introduction to binary number systems and Boolean algebra, and deal with various basal circuit and control elements. Finally, students will gain an insight into robotics with a focus on industrial robots. In this context, the students learn the description and calculation of positions and movements of individual limbs of a robot arm.

Course Outcomes

On successful completion, students will be able to

- understand the basic aspects of automation.
- understand the different sizes and units in measurement technology.
- differentiate between different measurement methods.
- understand the basic structure of measuring equipment.
- select a suitable sensor based on various criteria.
- understand the elements of control systems.
- describe the behavior of control systems in the time and frequency domain.
- understand the basic principles of control technology.
- convert between different number systems and apply Boolean algebra.
- understand the structure of switching networks, plants, and storages.
- understand important elements of control systems such as signal generators and power amplifiers.
- design simple programmable logic controllers.
- understand the basic structure of industrial robots.
- calculate different movements and positions of jointed-arm robots.

Contents

1. Basics of Automation
    1.1 Basic Terms

- 1.2 Economic Aspects
- 1.3 Automation Pyramid
- 1.4 Measuring, Control, and Regulation Systems

2. Fundamentals of Measurement Technology
   - 2.1 Measurands and Units
   - 2.2 Forms of Measurement Signals
   - 2.3 Measurement Techniques
   - 2.4 Measuring Equipment
   - 2.5 Evaluation of Measurements and Measurement Errors

3. Sensors
   - 3.1 Function and Elements of Sensors
   - 3.2 Criteria for the Selection of Sensors
   - 3.3 Proximity Switches
   - 3.4 Photoelectric Sensors
   - 3.5 Ultrasonic Sensors
   - 3.6 Rotary Encoder
   - 3.7 Force, Torque, and Pressure Gauges
   - 3.8 Temperature Sensors
   - 3.9 Image Processing Sensors

4. Basics of Control Engineering
   - 4.1 Elements of Control Systems
   - 4.2 Structure Description
   - 4.3 Static Behavioral Description
   - 4.4 Behavioral Description in the Time Domain
   - 4.5 Behavioral Description in the Frequency Domain
   - 4.6 Practical examples

5. Basics of Control Technology
   - 5.1 Basic Principle and Elements of Control Systems
   - 5.2 Numerical Representations
   - 5.3 Boolean Algebra
   - 5.4 Switching Networks, Plants, and Storage Facilities
   - 5.5 Signal Generators and Power Amplifiers
   - 5.6 Programmable Logic Controllers
   - 5.7 Connection-Programmed Controls

6. Introduction to Robotics
   - 6.1 Terms and Classification
   - 6.2 Basic Elements
   - 6.3 Classification of Robots

7. Kinematics of a Robot
   - 7.1 Coordinate Systems and Reference Points
   - 7.2 Rotations
   - 7.3 Forward and Reverse Transformations
   - 7.4 Denavit-Hartenberg Transformation

Literature

Compulsory Reading

Further Reading

- Gardner, R. (2021). Introduction to plant automation and controls. Taylor & Francis.
- Jazar, R. (2010). Theory of applied robotics: Kinematics, dynamics, and control (2nd ed.). Springer.
- Moir, T. (2020). Feedback. Springer.
- Morris, A. S., & Langari, R. (2020). Measurement and instrumentation: Theory and application (3rded.). Academic Press.
- Tse, F. S., & Morse, I. E. (2009). Measurement and instrumentation in engineering. CRC Press.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions		

Mobile Software Engineering

Module Code: DLBCSEMSE

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. jan Rüterbories (Mobile Software Engineering) / Dr. Christian Remfert (Project: Mobile Software Engineering)

Contributing Courses to Module

- Mobile Software Engineering (DLBCSEMSE01)
- Project: Mobile Software Engineering (DLBCSEMSE02)

Module Exam Type

Module Exam	Split Exam
	Mobile Software Engineering • Study Format "On Campus": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Mobile Software Engineering • Study Format "myStudies": Written Assessment: Project Report • Study Format "On Campus": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Mobile Software Engineering

- Basics of mobile software development
- Android system architecture
- Development environment
- Core components of an Android app
- Interaction between application components
- Advanced techniques

Project: Mobile Software Engineering

Conception, implementation, and documentation of small, mobile applications on the basis of a concrete task.

Learning Outcomes

Mobile Software Engineering

On successful completion, students will be able to

- recognize the differences and peculiarities of software development for mobile systems and explain them.
- differentiate between different activities, roles, and risks in the creation, operation, and maintenance of mobile software systems.
- explain and differentiate between the architecture and technical features of the Android platform.
- independently create mobile software systems to solve concrete problems for the “Android” platform.

Project: Mobile Software Engineering

On successful completion, students will be able to

- independently design and create a prototype of a small mobile application to solve a specific problem.
- recognize typical problems and challenges in the practical implementation of small mobile applications.
- document the conception and implementation of small, independently designed and implemented mobile applications.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Mobile Software Engineering

Course Code: DLBCSEMSE01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using the mobile platform "Android" as an example, it will be demonstrated how the programming of mobile applications (apps) differs from the development of browser-based information systems, which technologies and programming concepts are typically used, and which typical challenges there are in app development for industrial applications.

Course Outcomes

On successful completion, students will be able to

- recognize the differences and peculiarities of software development for mobile systems and explain them.
- differentiate between different activities, roles, and risks in the creation, operation, and maintenance of mobile software systems.
- explain and differentiate between the architecture and technical features of the Android platform.
- independently create mobile software systems to solve concrete problems for the “Android” platform.

Contents

1. Basics of Mobile Software Development
   - 1.1 Special Features of Mobile Devices
   - 1.2 Special Features of Mobile Software Development
   - 1.3 Classification of Mobile Devices
   - 1.4 The Android Platform
2. Android System Architecture
   - 2.1 The Android System
   - 2.2 Safety and Security
   - 2.3 Communication with Networks
3. Development Environment
   - 3.1 Android Studio
   - 3.2 First App and Emulator Test

3.3 Application Deployment

4. Core Components of an Android App
   - 4.1 Overview of the Components of an Android App
   - 4.2 Activities, Layouts, and Views
   - 4.3 Resources
   - 4.4 Summary in an App
   - 4.5 Graphic Design

5. Interaction Between Application Components
   - 5.1 Intents
   - 5.2 Services
   - 5.3 Broadcast Receiver

6. Advanced Techniques
   - 6.1 Threading
   - 6.2 Application Memory

Literature

Compulsory Reading

Further Reading

- Allen, G. (2021). Android for absolute beginners: Getting started with mobile apps development using the Android Java SDK. Apress.
- Boyer, R., & Mew, K. (2016). Android application development cookbook (2nd ed.). Packt Publishing.
- Collins, L., & Ellis, R. S. (2015). Mobile devices: Tools and technologies. CRC Press.
- Hagos, T. (2020): Learn Android Studio 4: Efficient Java-Based Android Apps Development. Berkeley, CA: Apress.
- Meike, B. G., & Schiefer, L. (2022). Inside the Android OS: Building, customizing, managing, and operating Android system services. Pearson.

Study Format On Campus

Study Format	Course Type
On Campus	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods
Tutorial Support ☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Mobile Software Engineering

Course Code: DLBCSEMSE02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using the knowledge gained in the course "Mobile Software Engineering using the Android platform as an example", students independently create a mobile application and document its conception and implementation.

Course Outcomes

On successful completion, students will be able to

- independently design and create a prototype of a small mobile application to solve a specific problem.
- recognize typical problems and challenges in the practical implementation of small mobile applications.
- document the conception and implementation of small, independently designed and implemented mobile applications.

Contents

- Conception, implementation, and documentation of small, mobile applications on the basis of a concrete task. Possible topics are, for example:
- A radio app to improve the exchange between listeners and stations in general, and listeners and radio presenters in particular.
- An app that allows a group of board game fans to better organize their regular evening game.
- An app that theses supervisors at IUBH can use to improve their supervision processes.

Literature

Compulsory Reading

Further Reading

- Allen, G. (2021): Android for Absolute Beginners [electronic resource]: Getting Started with Mobile Apps Development Using the Android Java SDK. Berkeley, CA: Apress.
- Boyer, R. & Mew, K. (2016): Android Application Development Cookbook - Second Edition. Birmingham, UK : Packt Publishing.
- Hagos, T. (2020): Learn Android Studio 4: Efficient Java-Based Android Apps Development. Berkeley, CA: Apress.

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format On Campus

Study Format	Course Type
On Campus	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Career Development

Module Code: DLBKAENT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Annette Strauß (Personal Career Plan) / Prof. Dr. Heike Schiebeck (Personal Elevator Pitch)

Contributing Courses to Module

- Personal Career Plan (DLBKAENT01_E)
- Personal Elevator Pitch (DLBKAENT02_E)

Module Exam Type

Module Exam	Split Exam
	Personal Career Plan • Study Format "Duales myStudium": Advanced Workbook • Study Format "myStudies": Advanced Workbook • Study Format "Distance Learning": Advanced Workbook Personal Elevator Pitch • Study Format "Duales myStudium": Concept Presentation • Study Format "Distance Learning": Concept Presentation • Study Format "myStudies": Concept Presentation

Weight of Module
see curriculum

Module Contents

Personal Career Plan

- Career Theories and Models
- Career Development
- Choosing Possible Careers
- Personal Branding
- Career Strategy
- Global Careers
- Employment Search

Personal Elevator Pitch

Through the application of self-reflection, self-awareness based on relevant career success parameters students should develop career goals, career stages, and their career strategy. Taking into account their current professional and/or study situation, the central elements of a short-, and medium-term career planning are worked out by the students for their individual case. At the end of the course, students will be able to present their personal elevator pitch and communicate it in a proper way that is appropriate for the target group or audience. In this way, they will reflect on their current professional situation. The personal elevator pitch, being at hear of personal branding, supports the conveyance of this vision during personal networking activities.

Learning Outcomes

Personal Career Plan

On successful completion, students will be able to

- understand, apply, and reflect presented career theory and models with regard to their personal situation to arrive at a concept or pictore of a desired career.
- understand and critically reflect the concept of career and career planning.
- understand the relevance of a strategically oriented career planning.
- understand the importance of and conduct a personal assessment to identify one's personality, values, motivation, strengths, competencies, skills, and interests.
- understand the necessity of building and maintaining their own personal brand.
- understand differing job search processes across national/international contexts, and to create context-sensitive job applications accordingly.
- understand the principles of global careers and how to effectively act in international environments.

Personal Elevator Pitch

On successful completion, students will be able to

- identify their career goals, career stages, and the personal status quo with regard to their achievement.
- reflect their current situation and define where they want to aim.
- develop a career strategy by creating personal career goals and a coherent action plan.
- understand and apply the process of building a personal brand.
- define their identity, skills, profession, reasons to believe and necessary investments.
- identify their personal strengths and their core driver.
- understand the power of effective communication, networking, and storytelling.
- understand the principles and apply the process of designing a strong personal elevator pitch.
- critically reflect and adapt their personal elevator pitch to the specificities of the context, audience, target group, and way of delivery.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Human Resources	All Bachelor Programs in the Human Resources field

Personal Career Plan

Course Code: DLBKAENT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In today's complex and ever-changing environment, the forms of careers vary depending on the context, understanding of values, and market dynamics. The 'classic career ladder' that one is climbing being the only predominant form of career is long outdated, and individuals are being confronted with a great number of opportunities regarding industry or job choice and working arrangements.Considering the great variety of options especially for well-educated individuals, has become more important than ever to make informed decisions. This course is designed to support students maneauvering themselves through these complexities of their personal career plan, whereby self-awareness, self-reflection, and goal-setting are important elements of this process. Guided by central elements of career theory, career models, and research outcomes, students will be given tools and reflection exercises to arrive at a solid, directly applicable strategy to further steet their professional progress and career steps.

Course Outcomes

On successful completion, students will be able to

- understand, apply, and reflect presented career theory and models with regard to their personal situation to arrive at a concept or pictore of a desired career.
- understand and critically reflect the concept of career and career planning.
- understand the relevance of a strategically oriented career planning.
- understand the importance of and conduct a personal assessment to identify one's personality, values, motivation, strengths, competencies, skills, and interests.
- understand the necessity of building and maintaining their own personal brand.
- understand differing job search processes across national/international contexts, and to create context-sensitive job applications accordingly.
- understand the principles of global careers and how to effectively act in international environments.

Contents

1. Career Theories and Approaches
    - 1.1 Traditional Career Theories and Models
    - 1.2 Protean Career Orientation
    - 1.3 Career Learning Cycle
2. Career Development

Literature
Compulsory Reading
Further Reading ▪ Baruch, Y. (2022). Managing Careers and Employability. SAGE. ▪ Greenhaus, J.H., Callanan, G.A., & Godshalk, V.M. (2018). Career Management for Life (5th edition). College of Business & Public Management Faculty Books. ▪ Hoeckstra, H. (2011). A career roles model of career development. Journal of Vocational Behavior, 78(2), 159-173. ▪ Ibarra, H. (2004). Working Identity: Unconventional Strategies for Reinventing Your Career. Harvard Business School Press. ▪ Kingsley, T. (2022). Personal Branding. Independently published. ▪ Ng, T.W.H., Eby, L.T., Sorensen, K.L., & Feldman, D.C. (2005). Predictors of objective and subjective career success: A meta-analysis. Personnel psychology, 58(2), 367-408. ▪ Ng, T.W.H., & Feldman, D.C. (2014). Subjective career success: A meta-analytic review. Journal of Vocational Behavior, 85(2), 169-179.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Advanced Workbook

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods

Tutorial Support
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Online Tests
- ☑ Guideline

Study Format myStudies

Study Format	**Course Type**
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Advanced Workbook

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Advanced Workbook

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Slides	

Personal Elevator Pitch

Course Code: DLBKAENT02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBKAENT01_E

Course Description

The forms of careers vary depending on the context or personal preferences in today's ever-changing, demanding, and complex environment. Changes in the environment, as for example technology, sustainability, and the rise of artificial intelligence, push individuals to take career transitions into their own hands. Personal endeavors to develop one's career through the acquisition of, for instance, new projects, jobs, or employers, require the right strategies to be successful. Contacts through targeted networking and the development of one's own brand play a special role here. Evenly so for individuals starting their careers after having accomplished their education, effective networking is key to career entry and development in these turbulent times. In addition, personal branding is a concept that not only has gained relevance in research but is also widely used in career counseling. Developing and conveying a personal brand is central to this course. Using the personal branding approach during networking activities, individuals can actively contribute to their career success.

Course Outcomes

On successful completion, students will be able to

- identify their career goals, career stages, and the personal status quo with regard to their achievement.
- reflect their current situation and define where they want to aim.
- develop a career strategy by creating personal career goals and a coherent action plan.
- understand and apply the process of building a personal brand.
- define their identity, skills, profession, reasons to believe and necessary investments.
- identify their personal strengths and their core driver.
- understand the power of effective communication, networking, and storytelling.
- understand the principles and apply the process of designing a strong personal elevator pitch.
- critically reflect and adapt their personal elevator pitch to the specificities of the context, audience, target group, and way of delivery.

Contents

- The core element of this course is a personal elevator pitch with the use of a personal branding canvas. The creation of a personal brand is not only relevant for self-employed freelancers or entrepreneurs but is as well helpful for individuals who strive for their own further development on the career ladder within their organization or for those who

are seeking employment. Having understood the characteristics of and reasoning behind personal branding and the underlying process, students will be able to apply this process to their own person and situation.
- Self-awareness being the main 'ingredient' for an effective personal brand, students will be encouraged to go on an intensive self-reflection journey to deepen their understanding of their identity, skills, profession, and reasons to believe for a personal brand, and subsequently, for a personal elevator pitch.
- Being at the heart of and the essence of personal branding, the elevator pitch enables individuals to impactfully present themselves in a nutshell to important individuals and potential employers. Having understood the principles and key success factors characterizing an elevator pitch, students will be able to develop their own one. They will learn to consider aspects like timing, benefit, clear positioning, target audience through an oral form of delivery. In addition, the role of communication, networking and storytelling principles will be highlighted.
- Knowledge of the core elements and success factors of the personal elevator pitch within the framework of the individual career development.

Literature

Compulsory Reading

Further Reading

- Dowling, D. (2009). How to Perfect an Elevator Pitch About Yourself. Harvard Business Review. https://hbr.org/2009/05/how-to-perfect-an-elevator-pit.
- Gorbatov, S., Khapova, S.N., & Lysova, E.I. (2018). Personal branding: Interdisciplinary systematic review and research agenda. Frontiers in psychology, 2238.
- Gorbatov, S., Khapova, S.N., & Lysova, E.I. (2019). Get noticed to get ahead: The impact of personal branding on career success. Frontiers in psychology, 2662.
- Jourdan Jr., Louis F., Deis, M., & Lysova, E.I. (2010). Getting Your Elevator Pitch To The Plate. Business Journal for Entrepreneurs, 2010(1), 43-47.
- Woodside, A.G. (2010). Brand consumer storytelling theory and research: Introduction to a Psychology & Marketing special issue. Psychology & Marketing, 27(6), 531-540.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Concept Presentation

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Concept Presentation

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	**Course Type**
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Concept Presentation

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Microsoft ERP- Dynamics 365 Business Central - Functional Consultant

Module Code: DLBMSERP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Sebastian Werning (Project: Dynamics 365 Business Central - Financial Company Setup) / Prof. Dr. Sebastian Werning (Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution)

Contributing Courses to Module

- Project: Dynamics 365 Business Central - Financial Company Setup (DLBMSERP01)
- Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution (DLBMSERP02)

Module Exam Type

Module Exam	Split Exam Project: Dynamics 365 Business Central - Financial Company Setup • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report
Weight of Module see curriculum	

Module Contents

Project: Dynamics 365 Business Central - Financial Company Setup

This module empowers students to configure and perform core business processes of a small or medium-sized company in an enterprise resource planning (ERP) system using Microsoft Dynamics 365 Business Central. Therefore, the module will address the core financial setup as well as sales and distribution processes for a small or medium-sized company.

Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution

This module empowers students to configure and perform core business processes of a small or medium-sized company in an enterprise resource planning (ERP) system using Microsoft Dynamics 365 Business Central. Therefore, the module will address the core financial setup as well as sales and distribution processes for a small or medium-sized company.

Learning Outcomes

Project: Dynamics 365 Business Central - Financial Company Setup

On successful completion, students will be able to

- describe the core feature of Business Central as an ERP system for small or medium-sized company.
- initially setup Business Central (SaaS).
- configure a new small or medium-sized demo company in Business Central.
- manage core security settings in Business Central.
- configure financials by setting up the finance module in Business Central.
- configure the chart of accounts in Business Central.

Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution

On successful completion, students will be able to

- configure sales module in Business Central.
- configure purchasing module in Business Central.
- set up inventory management in Business Central.
- configure master data for sales and purchasing in Business Central.
- describe how to perform Business Central operations including selling and purchasing.
- process financial documents.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Project: Dynamics 365 Business Central - Financial Company Setup

Course Code: DLBMSERP01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course aims to empower students to perform financial business processes of a small or medium-sized company using the well-established cloud-based ERP system Microsoft Dynamics 365 Business Central (BC). At first, you will gain important insights into the typical structure of BC. Based on that knowledge, you will be guided to setup a SaaS environment for a demo company in BC. To ensure a safe operation of BC in the cloud you will learn how to configure essential security settings. Next, you will familiarize yourself with the most important and common financial business processes for a small or medium-sized business. Finally, you will configure the accounting module for your demo company in BC.

Course Outcomes

On successful completion, students will be able to

- describe the core feature of Business Central as an ERP system for small or medium-sized company.
- initially setup Business Central (SaaS).
- configure a new small or medium-sized demo company in Business Central.
- manage core security settings in Business Central.
- configure financials by setting up the finance module in Business Central.
- configure the chart of accounts in Business Central.

Contents

- Embarking on the journey of utilizing BC involves a series of pivotal steps. It commences with the fundamental task of setting up the platform itself. This encompasses the creation and meticulous configuration of a company, including the setup of security settings to ensure a secure operational environment. The process further extends to establishing the core functionality, which serves as the backbone of operations. The inclusion of dimensions adds an additional layer of precision to data handling. A critical aspect of the BC framework lies in managing approvals seamlessly through the implementation of workflows, streamlining processes and enhancing efficiency. Within the finance module, a thorough configuration is undertaken. This involves the setup of financial management procedures, which ensures the financial aspect of operations is well-structured and organized. Part of this process includes the establishment of the chart of accounts, providing a foundation for accurate

financial tracking. Moreover, the setup of posting groups refines the financial recording process, facilitating precise categorization. The establishment of journals and bank accounts enhances financial transparency, offering a clear overview of monetary transactions. Notably, payable accounts are configured, ensuring seamless management of outgoing payments. Similarly, the setup of receivable accounts streamlines the handling of incoming payments. Collectively, these steps form a comprehensive roadmap to unleash the full potential of BC, enabling efficient operations and meticulous financial management.

Literature

Compulsory Reading

Further Reading

- Gayer, M., Hauptmann, C., & Ebert, J. (2020). Microsoft Dynamics 365 Business Central: Das Anwenderbuch zur Abwicklung von Geschäftsprozessen (11. Ausgabe). Carl Hanser Verlag.
- Ferner, C. (2020): Microsoft Dynamics 365 Business Central Basiswissen (Auflage 1). BoD – Books on Demand.
- Merk, J. (2020). Microsoft Dynamics 365 BC Finanzbuchhaltung. NEW ERA Publications
- Microsoft Corporation. (2023). Learning path for certification: Dynamics 365 Business Central Functional Consultant.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution

Course Code: DLBMSERP02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBMSERP01

Course Description

This course aims to empower students to perform sales and distribution processes using the well-established cloud-based ERP system Microsoft Dynamics 365 Business Central (BC). At first, you will gain important insights into the configuration of the sales module for a small or medium-sized company. Based on that knowledge, you will be guided to setup the purchasing module and inventory management in BC. Next, you will familiarize yourself with the configuration of the corresponding master data management. Finally, you will perform common business transaction in the sales and distribution module as well as process core financial documents for your demo company in BC.

Course Outcomes

On successful completion, students will be able to

- configure sales module in Business Central.
- configure purchasing module in Business Central.
- set up inventory management in Business Central.
- configure master data for sales and purchasing in Business Central.
- describe how to perform Business Central operations including selling and purchasing.
- process financial documents.

Contents

- To ensure the smooth flow of business processes in BC, various steps are necessary. First, the configuration of the sales and purchases modules takes place to establish the foundation for efficient work. During this phase, inventory management is set up to ensure an organized inventory flow. An essential step is configuring master data for sales and purchasing, as these form the basis for all subsequent activities. Prices and discounts are also established to create a clear pricing structure. Following this, common operations are performed in Business Central, encompassing both basic tasks and frequent operations. The processing of purchases as well as the handling of sales transactions is a central part of the process and a common operation in BC. Financial documents are processed as well to accurately represent the accounting aspect. Another step involves processing payments and journal entries to meticulously manage the financial aspects. All of these steps contribute to the seamless execution of business activities while maintaining financial integrity.

Literature
Compulsory Reading
Further Reading ▪ Gayer, M., Hauptmann, C., & Ebert, J. (2020). Microsoft Dynamics 365 Business Central: Das Anwenderbuch zur Abwicklung von Geschäftsprozessen (11. Ausgabe). Carl Hanser Verlag. ▪ Ferner, C. (2020): Microsoft Dynamics 365 Business Central Basiswissen (Auflage 1). BoD – Books on Demand. ▪ Microsoft Corporation. (2023). Learning path for certification: Dynamics 365 Business Central Functional Consultant.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

SAP - SAP S/4HANA Business Process Integration - Application Associate

Module Code: DLBSAPBPI

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Sebastian Werning (Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management) / Prof. Dr. Sebastian Werning (Project: SAP S/4HANA - Business Processes)

Contributing Courses to Module

- Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management (DLBSAPBPI01)
- Project: SAP S/4HANA - Business Processes (DLBSAPBPI02)

Module Exam Type

Module Exam	Split Exam Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report Project: SAP S/4HANA - Business Processes • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report
Weight of Module see curriculum	

Module Contents

Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management

This module empowers students to configure and perform core business processes of medium-sized and large companies in an enterprise resource planning (ERP) system using SAP S/4HANA and the user interface SAP Fiori. The module consists of two steps, each catering to specific facets. In the first step, attention is directed towards the core financial setup as well as the preliminary configuration of the Human Capital Management module using a demo company as an illustration. This step lays down a robust foundation in these domains. Moving on to the second step, the focus shifts to expanding the initial setup by integrating business processes related to sales, distribution, and production.

Project: SAP S/4HANA - Business Processes

Learning Outcomes

Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management

On successful completion, students will be able to

- navigate confidently within the SAP S/4HANA ERP system.
- explain the organizational structures.
- understand the concept of master data.
- explain financial accounting (FI) module.
- explain management accounting (CO) module.
- explain the employee master data record (HCM).

Project: SAP S/4HANA - Business Processes

On successful completion, students will be able to

- describe the source to pay business process (MM).
- describe warehouse management systems (WM).
- explain the design to operate business process (PP).
- describe the order to cash business process (SD).
- create a project structure (PS).
- defining the organizational levels used in enterprise asset management (EAM).

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology fields

Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management

Course Code: DLBSAPBPI01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course aims to empower students to perform financial business processes of medium-sized and large companies using the well-established ERP system SAP S/4HANA (S4H). At first, you will gain important insights into the typical organizational structure and navigation within S4H. You will understand the new user experience concept of SAP Fiori. Based on that knowledge, you will get in contact with the concept of master data in S4H. Next, you will familiarize yourself with the most important and common financial business processes in the financial accounting (FI) and management accounting (CO) module of S4H. Finally, you will configure the employee master data record in the Human Capital Management (HCM) module of S4H.

Course Outcomes

On successful completion, students will be able to

- navigate confidently within the SAP S/4HANA ERP system.
- explain the organizational structures.
- understand the concept of master data.
- explain financial accounting (FI) module.
- explain management accounting (CO) module.
- explain the employee master data record (HCM).

Contents

- The course provides a comprehensive introduction into SAP S/4HANA starting with the overall SAP S/4HANA Enterprise Management: Overview. Therefore, the course offers a comprehensive and presentation of various key concepts and functions relevant in the world of SAP S/4HANA. Furthermore, it focuses on the new user experience brought by SAP Fiori UX. The course covers the basics of SAP S/4HANA as well as the various organizational structures that exist within this system. A central concept addressed is that of master data. The subjects of Financial Accounting and Management Accounting (Record-to-Report processing) are thoroughly examined, providing an overview. Within these areas, Financial Accounting (FI) is explained, and Management Accounting (CO) is illuminated further. The integration between FI and CO is also outlined. The fundamentals of Financial Accounting and Management Accounting (Record-to-Report processing) are further delved into. This includes the definitions of General Ledger (G/L) accounts and cost elements, as well as

the definition of cost centers. Step-by-step instructions for posting G/L account documents and handling business partners and invoices are conveyed. The management of Asset Accounting, Activity Types, and Internal Orders is also comprehensively explained. The course also addresses the realm of Human Capital Management (HCM). This covers organizational management in HCM, as well as the significance of HCM master data. Another important aspect is the integration with SAP Success Factors.

Literature

Compulsory Reading

Further Reading

- Fitzner, W., Fitzner, D. (2021). SAP S/4HANA: Der Grundkurs für Einsteiger und Anwender. SAP Press
- Fix, W., Plota, R. (2021). SAP – Der technische Einstieg: Der Standardtitel für Ausbildung, Studium und Quereinstieg. SAP Press
- SAP SE. (2023). SAP Learning journey "Explore Integrated Business Processes in SAP S/4HANA".
- SAP SE. (2023). SAP Learning journey "Discovering End-to-End Business Processes for the Intelligent Enterprise".

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: SAP S/4HANA - Business Processes

Course Code: DLBSAPBPI02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBSAPBPI01

Course Description

This course aims to empower students to perform sales and distribution processes of medium-sized and large companies using the well-established ERP system SAP S/4HANA (S4H).At first, you will gain important insights into the configuration of the purchasing (MM) and warehouse management (WM) modulewithin S4H. You willalso understand the production process (PP) of S4H. Based on that knowledge, you willget in contact with the lead to cash business process (SD) in S4H. Next, you will familiarize yourself with the project system (PS) in S4H while creating project steps and structures. Finally, you will defining the organizational levels and for the management and maintenance of the company's physical assets in the enterprise asset management (EAM) module of S4H.

Course Outcomes

On successful completion, students will be able to

- describe the source to pay business process (MM).
- describe warehouse management systems (WM).
- explain the design to operate business process (PP).
- describe the order to cash business process (SD).
- create a project structure (PS).
- defining the organizational levels used in enterprise asset management (EAM).

Contents

- The course covers a wide range of processes and concepts within SAP S/4HANA: Purchase to Pay Processing in SAP S/4HANA: Exploring the Purchase to Pay business process, including the definition of master data involved. This encompasses creating vendor master records, listing vendor-specific master data records, generating purchase requisitions, crafting purchase orders, posting goods receipts for purchase orders, and managing vendor invoices. The automatic payment run process is also elucidated. Warehouse Management - Stock Transfer: This section delves into Warehouse Management (WM) structures and usage, highlighting the distinctions between Extended Warehouse Management (EWM), WM, and Inventory Management (IM). The process of handling stock transfer orders is outlined. Plan to Produce Business Process in SAP S/4HANA: Understanding the Plan to Produce process within SAP S/4HANA, which encompasses defining master data, creating product cost estimates, planning product demand through integrated planning, establishing Material Requirements Planning (MRP) processes, and executing advanced planning. Advanced

Planning - Describing the Manufacturing Business Process: Exploring the manufacturing business process, starting from the creation and release of production orders to material withdrawal, order confirmation, materials goods receipt, and period-end closing activities. Order to Cash Processing in SAP S/4HANA: This section focuses on the Order to Cash business process, describing the master data used in sales and distribution. The process involves creating customer master records, setting up condition records, processing sales orders, managing delivery documents, generating customer invoices, and handling related activities. Project System (PS): Detailing the steps within Project System, including creating project structures, project planning, budgeting, project execution, and concluding with period-end closing activities. SAP Enterprise Asset Management (EAM): Covering the business steps in SAP EAM, describing the master data utilized, creating notifications, processing maintenance orders, executing maintenance tasks, and wrapping up with period-end closing activities.

Literature

Compulsory Reading

Further Reading

- Fitzner, W., Fitzner, D. (2021). SAP S/4HANA: Der Grundkurs für Einsteiger und Anwender. SAP Press
- Fix, W., Plota, R. (2021). SAP – Der technische Einstieg: Der Standardtitel für Ausbildung, Studium und Quereinstieg. SAP Press
- SAP SE. (2023). SAP Learning journey “Explore Integrated Business Processes in SAP S/4HANA”.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

AWS Cloud Specialization

Module Code: DLBAWSCLSP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Georgi Dimchev (Project: AWS - Cloud Essentials) / Prof. Dr. Tianxiang Lu (Project: AWS - Cloud Advanced)

Contributing Courses to Module

- Project: AWS - Cloud Essentials (DLBPAWSCLES01)
- Project: AWS - Cloud Advanced (DLBPAWSCLAD01)

Module Exam Type

Module Exam	Split Exam
	Project: AWS - Cloud Essentials • Study Format "myStudies": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report Project: AWS - Cloud Advanced • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report

Weight of Module
see curriculum

Module Contents

Project: AWS - Cloud Essentials

Students will learn the foundational concepts and services of Amazon Web Services (AWS), covering its core infrastructure services including computing, storage, and networking through practical experience. Emphasis is placed on practical skills for deploying Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions.

Project: AWS - Cloud Advanced

This course offers advanced understanding of AWS, with a particular emphasis on specialized areas such as Solutions Architecture, Compliance & Security, and AI & Machine Learning. Students will acquire hands-on expertise in these areas, with the goal of enabling them to deploy laaS, Paas, or SaaS workloads using AWS, effectively tackle real-life interdisciplinary challenges, and confidently handle service configurations within the AWS cloud console.

Learning Outcomes

Project: AWS - Cloud Essentials

On successful completion, students will be able to

- understand the core services of AWS including compute, network, databases, and storage, deployment models (on-premises, hybrid, and vpc).
- explain the shared responsibility model, describe the basic global infrastructure and core security services.
- describe the AWS Well-Architected Framework and the basics of AWS Cloud Migration.
- get familiar with the terminology and concepts related to AWS Services, the AWS Management Console, AWS security measures, IAM and AWS networking services.
- apply and manage core service settings within the AWS cloud console effectively.
- assess data storage services in AWS to meet various application needs.
- plan and implement a scenario-based serverless service for small or medium-sized companies.
- configure basic network security using Amazon CloudWatch monitoring features for simple use cases in AWS, ensuring secure cloud operations.
- critically examine the core billing, account management, and pricing models and explain how to use pricing tools to make cost-effective choices for AWS services.

Project: AWS - Cloud Advanced

On successful completion, students will be able to

- understand and articulate the core services provided by AWS within chosen specialization tracks, including Solutions Architect, Compliance & Security, and AI & Machine Learning.
- critically examine the pros and cons of developing and deploying real-world scenarios using AWS IaaS, PaaS, vs. SaaS and public, private or hybrid deployment demonstrating a clear grasp of the necessary service and deployment intricacies.
- manage and configure profound service settings within the AWS cloud console, showing depth in technical proficiency and operational capabilities.
- critically assess, test and monitor the effect of different AWS deployment features, addressing interdisciplinary challenges through the appropriate use of AWS cloud services in realistic use cases.
- assess and critically reflect on AWS-based solutions, considering industry compliance and security requirements, ensuring a robust understanding of the legal and regulatory framework.
- apply and implement machine learning and artificial intelligence concepts using AWS to solve real-world problems, demonstrating innovative thinking and practical application of theoretical knowledge.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Project: AWS - Cloud Essentials

Course Code: DLBPAWSCLES01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Amazon Web Services (AWS) is a comprehensive cloud computing platform provided by Amazon that offers scalable computing power, storage, and various other functionalities to help businesses and individuals deploy applications and manage data efficiently. It reduces the need for physical hardware, thus lowering costs and increasing flexibility by allowing users to access services and resources on-demand from anywhere in the world. This service is highly relevant for daily life and business as it supports a wide range of applications and services, from hosting websites to supporting IoT devices and big data analytics, ultimately facilitating innovation, scalability, and global operations.This course prepares students for the AWS Cloud Practitioner Certificate, providing a foundational understanding of AWS core services. Students will learn to articulate the benefits and use cases of AWS IaaS, PaaS, and SaaS, and grasp the basics of public, private, and hybrid cloud deployments. The course emphasizes practical skills in managing and configuring AWS services, ensuring students can effectively navigate the AWS cloud console. It lays the groundwork for critical assessments of AWS deployment features, addressing compliance and security requirements, and preparing students for more advanced AWS certifications and applications

Course Outcomes

On successful completion, students will be able to

- understand the core services of AWS including compute, network, databases, and storage, deployment models (on-premises, hybrid, and vpc).
- explain the shared responsibility model, describe the basic global infrastructure and core security services.
- describe the AWS Well-Architected Framework and the basics of AWS Cloud Migration.
- get familiar with the terminology and concepts related to AWS Services, the AWS Management Console, AWS security measures, IAM and AWS networking services.
- apply and manage core service settings within the AWS cloud console effectively.
- assess data storage services in AWS to meet various application needs.
- plan and implement a scenario-based serverless service for small or medium-sized companies.
- configure basic network security using Amazon CloudWatch monitoring features for simple use cases in AWS, ensuring secure cloud operations.
- critically examine the core billing, account management, and pricing models and explain how to use pricing tools to make cost-effective choices for AWS services.

Contents

- This course offers a comprehensive exploration of Amazon Web Services (AWS), focusing on its core services such as computing, networking, databases, and storage solutions. Students will delve into the AWS shared responsibility model, understand the global infrastructure, and learn about the integral security services provided. This also covers the AWS Well-Architected Framework and an introduction of the fundamentals for cloud migration strategies. Through hands-on exercises, students will gain proficiency in managing AWS environments using the AWS Management Console and implement security measures via AWS Identity and Access Management (IAM) and network services. Additionally, the course emphasizes the importance of cost management, enabling students to critically analyze AWS pricing models to make informed financial decisions for cloud-based solutions.

Literature

Compulsory Reading

Further Reading

- AWS Training and Certification Skill Builder. (2024). AWS Cloud Practitioner Essentials (7 hours).
- AWS Training and Certification Skill Builder. (2024). AWS Cloud Quest: Cloud Practitioner.
- AWS Training and Certification Skill Builder. (2024). AWS Technical Essentials (4 hours).
- AWS Training and Certification Skill Builder. (2024). Serverless – Knowledge Badge Readiness Path (13 hours).
- AWS Training and Certification Skill Builder. (2024). Standard Exam Prep Plan: AWS Certified Cloud Practitioner (CLF-C02) (18 hours).

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: AWS - Cloud Advanced

Course Code: DLBPAWSCLAD01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

AWS (Amazon Web Services) is a comprehensive cloud computing platform provided by Amazon that offers scalable computing power, storage, and various other functionalities to help businesses and individuals deploy applications and manage data efficiently. It reduces the need for physical hardware, thus lowering costs and increasing flexibility by allowing users to access services and resources on-demand from anywhere in the world. This service is highly relevant for daily life and business as it supports a wide range of applications and services, from hosting websites to supporting IoT devices, big data analytics and machine learning, ultimately facilitating innovation, scalability, and global operations. The course prepares students for the AWS Cloud Solution Architect Professional Certificate. It dives deeper into AWS core services, focusing on sophisticated deployment and management techniques. Students will critically examine and apply real-world scenarios using AWS IaaS, PaaS, and SaaS, and navigate complex deployment models. They will gain technical proficiency in managing advanced service settings within the AWS cloud console and address interdisciplinary challenges through hands-on practice. Additionally, the course covers assessing AWS solutions for compliance and security, ensuring robust understanding of legal frameworks. Students will also implement machine learning and AI concepts to solve real-world problems, fostering innovative thinking and practical application, and preparing them for the dynamic demands of the tech industry.

Course Outcomes

On successful completion, students will be able to

- understand and articulate the core services provided by AWS within chosen specialization tracks, including Solutions Architect, Compliance & Security, and AI & Machine Learning.
- critically examine the pros and cons of developing and deploying real-world scenarios using AWS IaaS, PaaS, vs. SaaS and public, private or hybrid deployment demonstrating a clear grasp of the necessary service and deployment intricacies.
- manage and configure profound service settings within the AWS cloud console, showing depth in technical proficiency and operational capabilities.
- critically assess, test and monitor the effect of different AWS deployment features, addressing interdisciplinary challenges through the appropriate use of AWS cloud services in realistic use cases.
- assess and critically reflect on AWS-based solutions, considering industry compliance and security requirements, ensuring a robust understanding of the legal and regulatory framework.
- apply and implement machine learning and artificial intelligence concepts using AWS to solve real-world problems, demonstrating innovative thinking and practical application of theoretical knowledge.

Contents

- This course ensures students gain a comprehensive understanding of AWS, specializing in Solutions Architect, Compliance & Security, and AI & Machine Learning. They will articulate core AWS services and critically examine the pros and cons of deploying real-world scenarios using AWS IaaS, PaaS, SaaS, and different deployment models (public, private, hybrid).
- Students will manage and configure service settings within the AWS cloud console, demonstrating technical proficiency. They will assess, test, and monitor AWS deployment features, addressing interdisciplinary challenges using realistic use cases. Additionally, students will evaluate AWS-based solutions for industry compliance and security, understanding the legal and regulatory frameworks.
- The course also covers applying machine learning and AI concepts using AWS to solve real-world problems, encouraging innovative thinking and practical application. This approach prepares students to excel in cloud architecture, compliance protocols, security measures, and AI-driven problem-solving, ensuring readiness for the tech industry's dynamic demands.

Literature
Compulsory Reading
Further Reading ▪ AWS Training and Certification Skill Builder. (2024). AWS Solutions Architect – Knowledge Badge Readiness Path (51 hours). ▪ AWS Training and Certification Skill Builder. (2024). Generative AI Learning Plan for Developers (12 hours). ▪ AWS Training and Certification Skill Builder. (2024). Online Course Supplement: Practical Data Science with Amazon SageMaker (1 day).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

AI Prompting Techniques and Process Innovation with Copilot

Module Code: DLBEAIPTPICOP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Knut Linke (Project: AI Excellence with Creative Prompting Techniques) / N.N. (Project: Process Innovation with Copilot)

Contributing Courses to Module

- Project: AI Excellence with Creative Prompting Techniques (DLBPKIEKPT01_E)
- Project: Process Innovation with Copilot (DLBPPICOP01)

Module Exam Type

Module Exam	Split Exam
	Project: AI Excellence with Creative Prompting Techniques • Study Format "myStudies": Oral Project Report • Study Format "Duales myStudium": Oral Project Report • Study Format "Distance Learning": Oral Project Report Project: Process Innovation with Copilot • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module
see curriculum

Module Contents

Project: AI Excellence with Creative Prompting Techniques

In this module, the students delve into the world of generative AI applications, creating AI-generated content like text, images, and videos, while learning to use, analyze, and evaluate these systems in their respective study fields.

Project: Process Innovation with Copilot

In this course, students will deepen their understanding and skills in working with Microsoft Copilot, an advanced tool for supporting various work processes through automation, text generation, and data analysis. A special focus will be placed on the ethical and data protection challenges that can arise when using such technologies.

Learning Outcomes

Project: AI Excellence with Creative Prompting Techniques

On successful completion, students will be able to

- comprehend and apply basic prompting techniques in generative AI applications.
- analyze and evaluate the effectiveness of the basic prompts.
- apply ethical considerations to the design and use of AI for basic prompting techniques.
- design, implement, and refine effective prompts to real-world scenarios through hands-on exercises.
- showcase creative and innovative thinking in the application of prompting techniques to solve complex problems in their field of studies.

Project: Process Innovation with Copilot

On successful completion, students will be able to

- understand the basic functions and applications of Microsoft Copilot, including in the fields of text generation and data analysis.
- recognize the possibilities for automating work processes using Copilot and its contribution to efficiency improvement.
- understand interdisciplinary collaboration with Copilot.
- identify and evaluate potential application areas of Copilot in a professional context.
- understand and discuss ethical and data protection aspects of using Copilot.
- develop a critical reflection on the advantages and disadvantages of using Copilot.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology field

Project: AI Excellence with Creative Prompting Techniques

Course Code: DLBPKIEKPT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students explore the fascinating world of prompting in generative AI applications. They engage in hands-on exercises to create new AI-generated content including text, images, and videos. Through these exercises, students learn how to effectively use, analyze, and evaluate these systems within their respective fields of study.

Course Outcomes

On successful completion, students will be able to

- comprehend and apply basic prompting techniques in generative AI applications.
- analyze and evaluate the effectiveness of the basic prompts.
- apply ethical considerations to the design and use of AI for basic prompting techniques.
- design, implement, and refine effective prompts to real-world scenarios through hands-on exercises.
- showcase creative and innovative thinking in the application of prompting techniques to solve complex problems in their field of studies.

Contents

- In this course, students work on a basic practical implementation of a generative AI use case by choosing from a selection provided in the complementary guideline. The course provides practical examples as learning materials and exercises with basic prompting techniques for open-source text, image, and video generation use cases. The exercises are designed to inspire and guide students in completing their own generative AI use case work, which includes a use case description, chosen prompting techniques, outcomes, and critical evaluations from both technical and ethical perspectives.

Literature
Compulsory Reading
Further Reading ▪ Dang, H., Mecke, L., Lehmann, F., Goller, S., & Buschek, D. (2022). How to prompt? Opportunities and challenges of zero- and few-shot learning for human-AI interaction in creative applications of generative models. arXiv. https://arxiv.org/pdf/2209.01390.pdf ▪ Eapen, T. T., Finkenstadt, D. J., Folk, J., & Venkataswamy, L. (2023). How generative AI can augment human creativity. Harvard Business Review, July–August, 56–64. ▪ Wei, J., Wang, X., Schuurmans, D., Bosma, M. Ichter, B., Xia, F., Chi, E. H., Le., Q. V., & Zhou, D. (2023). Chain-of-though prompting elicit reasoning in large language models. arXiv. https://arxiv.org/pdf/2201.11903.pdf

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: Process Innovation with Copilot

Course Code: DLBPPICOP01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The integration of Artificial Intelligence (AI) into everyday work is revolutionizing how we handle tasks, analyze information, and make decisions. Microsoft Copilot is at the forefront of this development, offering numerous opportunities to enhance efficiency through automation and intelligent data processing.In this course, students explore the diverse functions of Microsoft Copilot, familiarize themselves with its applications, and engage with the ethical and data protection issues it raises. Through practical application within the project, they are empowered to effectively use Copilot in various professional contexts, optimize processes, and develop innovative solutions for complex problems. The critical examination of the potential and limitations of this technology also promotes a deep understanding of the responsibility that comes with the use of AI.

Course Outcomes

On successful completion, students will be able to

- understand the basic functions and applications of Microsoft Copilot, including in the fields of text generation and data analysis.
- recognize the possibilities for automating work processes using Copilot and its contribution to efficiency improvement.
- understand interdisciplinary collaboration with Copilot.
- identify and evaluate potential application areas of Copilot in a professional context.
- understand and discuss ethical and data protection aspects of using Copilot.
- develop a critical reflection on the advantages and disadvantages of using Copilot.

Contents

- In this course, students engage deeply with Microsoft Copilot by exploring its applications in practical, real-world scenarios. Through independent experimentation, they learn how Copilot can contribute to the automation of routine tasks, generate complex texts, and perform extensive data analyses. As part of the course, students are encouraged to design their own projects where they use Copilot to solve specific challenges. Emphasis is also placed on the consideration of ethical principles and data protection regulations. By participating in the offered exchange opportunities, students can further develop their critical awareness of the social impacts of AI usage. This course lays the foundation

for a thorough understanding of the possibilities and limitations of AI-powered work processes and prepares students to responsibly handle the challenges of the digitalized work environment.

Literature

Compulsory Reading

Further Reading

- Khan, A. (2024). Introducing Microsoft Copilot for managers: Enhance your team's productivity and creativity with generative AI-powered assistant. Apress.
- Microsoft. (2024). Explore how to use Microsoft 365 Copilot.
- Microsoft. (2024). Official Microsoft 365 Copilot for Service documentation.
- Narayanaswamy, A. (2024). Microsoft Copilot for Windows 11: Understanding the AI-powered features in Windows 11. Apress.
- Stratton, J. (2024). Copilot for Microsoft 365: Harness the power of generative AI in the Microsoft apps you use every day. Apress.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
Tutorial Support ☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	**Exam Preparation** ☑ Guideline

Studium Generale V and VI

Module Code: DLBSGFUS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

(Studium Generale V) / (Studium Generale VI)

Contributing Courses to Module

- Studium Generale V (DLBSG05_E)
- Studium Generale VI (DLBSG06_E)

Module Exam Type

Module Exam	Split Exam
	Studium Generale V • Study Format "Distance Learning": See Selected Course Studium Generale VI • Study Format "Distance Learning": See Selected Course

Weight of Module

see curriculum

Module Contents

Studium Generale V

In principle, all IU bachelor courses can be selected as courses for the "Studium Generale", so that the content can be chosen from the entire breadth of the IU distance learning program.

Studium Generale VI

In principle, all IU bachelor courses can be selected as courses for the "Studium Generale", so that the content can be chosen from the entire breadth of the IU distance learning program.

Learning Outcomes

Studium Generale V

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- deepen one's own skills and abilities in a self-directed manner.
- look beyond the boundaries of their own area of expertise

Studium Generale VI

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- deepen one's own skills and abilities in a self-directed manner.
- look beyond the boundaries of their own area of expertise.

Links to other Modules within the Study Program	Links to other Study Programs of the University
It is a stand-alone offering with possible references to various required and elective modules	All IU Distance Learning Bachelor Programs

Studium Generale V

Course Code: DLBSG05_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In the course "Studium Generale IV", students deepen their knowledge in a self-selected subject area by completing an IU course outside their applicable curriculum. This gives them the opportunity to look beyond their own subject area and acquire further competencies. The associated option enables students to self-determine their study content to focus even more on issues relevant to them and/or to strengthen or develop selected competencies.

Course Outcomes

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- deepen one's own skills and abilities in a self-directed manner.
- look beyond the boundaries of their own area of expertise

Contents

- The course "Studium Generale IV" offers students the opportunity to take courses outside of their curriculum and the result can be credited as an elective subject. In principle, all IU bachelor courses that fulfill the following requirements can be chosen for this purpose:
  - They are not part of an integral part of the applicable mandatory curriculum.
  - They do not have admission requirements or students can prove that they have met the admission requirement.
- The examination of the selected courses must be taken in full and finally passed in order to be credited as part of the 'Studium Generale'.

Literature

Compulsory Reading

Further Reading

- See course description of the selected course

Study Format Distance Learning

Study Format	Course Type
Distance Learning	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods

Studium Generale VI

Course Code: DLBSG06_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In the course "Studium Generale IV", students deepen their knowledge in a self-selected subject area by completing an IU course outside their applicable curriculum. This gives them the opportunity to look beyond their own subject area and acquire further competencies. The associated option enables students to self-determine their study content to focus even more on issues relevant to them and/or to strengthen or develop selected competencies.

Course Outcomes

On successful completion, students will be able to

- apply acquired key competencies to issues in their field of study and/or in their professional environment.
- deepen one's own skills and abilities in a self-directed manner.
- look beyond the boundaries of their own area of expertise.

Contents

- The course "Studium Generale IV" offers students the opportunity to take courses outside of their curriculum and the result can be credited as an elective subject. In principle, all IU bachelor courses that fulfill the following requirements can be chosen for this purpose:
  - They are not part of an integral part of the applicable mandatory curriculum.
- The examination of the selected courses must be taken in full and finally passed in order to be credited as part of the 'Studium Generale'.

Literature

Compulsory Reading

Further Reading

- See course description of the selected course

Study Format Distance Learning

Study Format	Course Type
Distance Learning	See Selected Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	See Selected Course

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	0 h	0 h

Instructional Methods

Internship

Module Code: FSINTER

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	None		10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Andreas Simon (Internship)

Contributing Courses to Module

- Internship (FSINTER01)

Module Exam Type

Module Exam	Split Exam
Study Format: myStudies Internship Reflection Paper (passed / not passed) Study Format: Distance Learning Internship Reflection Paper (passed / not passed)	

Weight of Module

see curriculum

Module Contents

Internship according to the Internship Regulations of the IU.

Learning Outcomes

Internship

On successful completion, students will be able to

- apply skills and knowledge they have obtained previously during their study program in an entrepreneurial environment.
- develop his / her practical and analytical skills in order to improve his / her employability.
- have practical knowledge and learn to work within an organization.
- acquire a first deep insight into organizational structures and communication procedures.
- apply comminication skills, socials skills, problem solving, time and project management which will shape their general management skills.
- shape their personality with the help of the interdisciplinary nature of the course especially in the area of the key qualifications like interpersonal skills or intercultural skills.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
Builds on modules of the chosen degree program	All myStudies programs

Internship

Course Code: FSINTER01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
	English		10	None

Course Description

This module consists of two parts: (1) preparation tutorials and (2) the internship itself. During the preparation tutorials, students will learn about the intention of the internship and about the intellectual as well as social requirements of the working environment.

Course Outcomes

On successful completion, students will be able to

- apply skills and knowledge they have obtained previously during their study program in an entrepreneurial environment.
- develop his / her practical and analytical skills in order to improve his / her employability.
- have practical knowledge and learn to work within an organization.
- acquire a first deep insight into organizational structures and communication procedures.
- apply comminication skills, socials skills, problem solving, time and project management which will shape their general management skills.
- shape their personality with the help of the interdisciplinary nature of the course especially in the area of the key qualifications like interpersonal skills or intercultural skills.

Contents

- Internship according to the Internship Regulations of the IU.

Literature

Compulsory Reading

Further Reading

- Sweitzer, F. H. & King, M. A. (2009). The Successful Internship: Personal, Professional, and Civic Development. 3rd ed.. Cengage. ISBN: 0-495-59642-6.
- Kaser, K., Brooks, J. R. & Brooks, K. (2007). Making the Most of your Internship. Thomson. ISBN: 0-538-44432-0.

Study Format myStudies

Study Format	Course Type
myStudies	

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Internship Reflection Paper (passed / not passed)

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	300 h	300 h

Instructional Methods
Tutorial Support ☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions

Study Format Distance Learning

Study Format	Course Type
Distance Learning	

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Internship Reflection Paper (passed / not passed)

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	300 h	300 h

Instructional Methods
Tutorial Support ☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions

Bachelor Thesis

Module Code: DLBBT

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Degree Program Advisor (SGL) (Bachelor Thesis) / Degree Program Advisor (SGL) (Colloquium)

Contributing Courses to Module

- Bachelor Thesis (DLBBT01)
- Colloquium (DLBBT02)

Module Exam Type

Module Exam

Split Exam

Bachelor Thesis

- Study Format "myStudies": Bachelor Thesis
- Study Format "Distance Learning": Bachelor Thesis

Colloquium

- Study Format "myStudies": Colloquium
- Study Format "Distance Learning": Colloquium

Weight of Module

see curriculum

Module Contents

Bachelor Thesis

- Bachelor's thesis
- Colloquium on the bachelor's thesis

Colloquium

Learning Outcomes

Bachelor Thesis

On successful completion, students will be able to

- work on a problem from their major field of study by applying the specialist and methodological skills they have acquired during their studies.
- independently analyze selected tasks with scientific methods, critically evaluate them, and develop appropriate solutions under the guidance of an academic supervisor.
- record and analyze existing (research) literature appropriate to the topic of their bachelor's thesis.
- prepare a detailed written elaboration in compliance with scientific methods.

Colloquium

On successful completion, students will be able to

- present a problem from their field of study using academic presentation and communication techniques.
- reflect on the scientific and methodological approach chosen in their bachelor's thesis.
- demonstrate that they can actively answer subject-related questions from the subject experts (reviewers of the bachelor’s thesis).

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
All modules in the Bachelor program	All Bachelor Programs in distance learning

Bachelor Thesis

Course Code: DLBBT01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		9	none

Course Description

The aim and purpose of the bachelor's thesis is to successfully apply the subject-specific and methodological competencies acquired during the course of study in the form of an academic dissertation with a thematic reference to the major field of study. The content of the bachelor's thesis can be a practical-empirical or theoretical-scientific problem. Students should prove that they can independently analyze a selected problem with scientific methods, critically evaluate it, and work out proposed solutions under the subject-methodological guidance of an academic supervisor. The topic chosen by the student from their respective field of study should meet the acquired scientific competences, deepening their academic knowledge and skills in order to meet the future needs of the field.

Course Outcomes

On successful completion, students will be able to

- work on a problem from their major field of study by applying the specialist and methodological skills they have acquired during their studies.
- independently analyze selected tasks with scientific methods, critically evaluate them, and develop appropriate solutions under the guidance of an academic supervisor.
- record and analyze existing (research) literature appropriate to the topic of their bachelor's thesis.
- prepare a detailed written elaboration in compliance with scientific methods.

Contents

- The bachelor's thesis must be written on a topic that relates to the content of the respective major field of study. In the context of the bachelor's thesis, the problem, as well as the scientific research goal, must be clearly emphasized. The work must reflect the current state of knowledge of the topic to be examined by means of an appropriate literature analysis. The student must prove their ability to use the acquired knowledge theoretically and/or empirically in the form of an independent and problem-solution-oriented application.

Literature
Compulsory Reading
Further Reading ▪ Lipson, C. (2018). How to write a BA thesis. A practical guide from your first ideas to your finished paper (2nd ed.). University of Chicago Press. ▪ Turabian, K. L. (2013). A Manual for Writers of Research Papers, theses, and dissertations (8th ed.). University of Chicago Press. ▪ Selection of literature according to topic

Study Format myStudies

Study Format	Course Type
myStudies	Thesis Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Bachelor Thesis

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
270 h	0 h	0 h	0 h	0 h	270 h

Instructional Methods

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Thesis Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Bachelor Thesis

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
270 h	0 h	0 h	0 h	0 h	270 h

Instructional Methods

Colloquium

Course Code: DLBBT02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		1	none

Course Description

The colloquium will take place after the submission of the bachelor's thesis. This is done at the invitation of the experts. During the colloquium, students must prove that they have independently produced the content and results of the written work. The content of the colloquium is a presentation of the most important work contents and research results by the student as well as the answering of questions by experts.

Course Outcomes

On successful completion, students will be able to

- present a problem from their field of study using academic presentation and communication techniques.
- reflect on the scientific and methodological approach chosen in their bachelor's thesis.
- demonstrate that they can actively answer subject-related questions from the subject experts (reviewers of the bachelor's thesis).

Contents

- The colloquium includes a presentation of the most important results of the bachelor's thesis, followed by the student answering the reviewers' technical questions.

Literature

Compulsory Reading

Further Reading

- Subject specific literature chosen by the student

Study Format myStudies

Study Format	Course Type
myStudies	Thesis Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Colloquium

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
30 h	0 h	0 h	0 h	0 h	30 h

Instructional Methods

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Thesis Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Colloquium

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
30 h	0 h	0 h	0 h	0 h	30 h

Instructional Methods