Automatic generation of security tests and exploits

Opportunity for a 6-month internship

Security Research @ SAP Labs France
Sophia-Antipolis – France

Maintaining security is a constantly shifting task, and we need to respond with continuous learning and research. The portfolio of SAP Security Research contains those topics that we believe are most important for SAP's security future.
SAP's vision to secure business is built on 3 ideals: **Zero-Vulnerability**, to harden the software by eliminating vulnerabilities, **Defensible Application**, to enable the software to identify and prevent attacks, and **Zero-Knowledge**, to make any theft of data useless through encryption.
Considering these aspects, SAP Security Research covers the following focal areas: Anonymization for Big Data, Secure Internet of Things, Software security analysis, Open-source analysis, Deceptive application, Applied cryptography, Quantum technology, and Machine Learning as enabler for the next generation of security.

Security Research proposes a 6-month internship in its Sophia-Antipolis offices (Mougins, France).

INTERNSHIP TOPIC

SAP business applications depend on open-source software (OSS) components, and it is paramount to ensure that such components are secure and do not contain vulnerabilities. Careful analysis is necessary to protect both SAP customers and SAP itself from any harm that can result from the use of insecure and vulnerable OSS.

One element supporting this goal is to use software tools to automate the analysis of OSS usage. SAP Security Research has developed a tool (https://github.com/SAP/vulnerability-assessment-tool) that scans Java and Python applications, identifies insecure OSS components, assesses the security risk in application-specific contexts, and proposes mitigation actions. This tool is regularly used by hundreds of development teams across SAP, and represents one important building block of SAP's overall strategy regarding the secure use of OSS.

A key feature of this tool is to support developers in determining whether a vulnerable piece of code that is present in a dependency could be reached from the application. We use a combination of static and dynamic analysis to do so, relying on test-cases that the application developer might have coded. However, the effectiveness of this approach is dependent on the quality and coverage of the existing test suite.

This internship aims at investigating methods to automatically generate test cases with the goal of covering a given fragment of a dependency (in particular, vulnerable fragments). When this is not possible (because that part of the dependency is not reachable), it should be possible to obtain a measure of confidence.
The student will design and implement a proof-of-concept that will be applied to one or more sample cases taken from real SAP products or from open-source applications.

CANDIDATE PROFILE

- University Level: Last year of MSc or less if the student has a good profile
- Solid foundations in CS and a passion for well-designed, cleanly implemented software
- Interest in experimental research
- Good knowledge of one or more of the following languages: Java, Python, Go
- Experience with Git, Linux (bash), software testing
- Prior exposure to one or more of the following topics is desirable but not mandatory:
  - software analysis, symbolic execution, concolic testing, constraint-solving, model checking
- Fluency in English (working language)
- Good oral and written communication skills

Copyright/Trademark

INTERNSHIP CONTEXT

SAP

Founded in 1972, SAP has grown to become the world's leading provider of business software solutions. SAP is market leader in enterprise application software. The company is also the fastest-growing major database company. Globally, more than 77% of all business transactions worldwide touch an SAP software system. With more than 347.000 customers in more than 180 countries, SAP includes subsidiaries in all major countries. SAP is the world's largest inter-enterprise software company and the world's third-largest independent software supplier, overall. SAP solutions help enterprises of all sizes around the world to improve customer relationships, enhance partner collaboration and create efficiencies across their supply chains and business operations. SAP employs more than 98.600 people.

Security Research at SAP Labs France, Sophia Antipolis

Based at SAP Labs France Mougins, Security Research Sophia-Antipolis addresses the upcoming security needs, focusing on increased automation of the security life cycle and on providing innovative solutions for the security challenges in networked businesses, including cloud, services and mobile.

STANDARD INTERNSHIP PACKAGE

- *Salary*: depending on the length of the internship and your diploma.
- *Lunch*: SAP Labs France has a local cafeteria; interns contribute 2,63 €uro/lunch, like other SAP employees.
- *Holidays*: French Bank Holidays
  - January 1st; April 12th, April 13th, May 1st, May 8th, May 21st, June 1st, July 14th; August 15th, Nov 1st and 11th; December 25th
- *Travel*: no trip will be paid by SAP.
- *Accommodation*: SAP can propose an accommodation for the duration of your internship. The accommodation is subsidized by SAP: the intern pays half of the rental cost: 342€ for a 1-room apartment or 442€ for a 2-room apartment (Choice depending on the availability).

CONTACTS AND PROCEDURE

Please candidate by clicking on this link:
https://career5.successfactors.eu/sfcareer/jobreqcareer?jobId=234527&company=SAP&username=

UPLOAD (all documents must be in English):

- Your CV
- Cover letter
- Any relevant documents