Differential Privacy Budget Optimization in Transfer Learning

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

According to the principles governing data protection regulations, personal data can be used for training machine learning models as soon as this finality is compatible with the purposes for which data has been collected. However, recent research has shown that that the training data, a subset of it, or information about who was in the training set, can in certain cases be reconstructed from models leading to data breaches [1,2].

Anonymization with differential privacy offers provable guarantees against re-identification and membership inference attacks. During the internship the student will investigate how to maintain data utility and to preserve privacy when training deep learning models. Building on previous results [3], new experiments to find how to reduce privacy budget consumption during training will be designed. These will employ transfer learning, for instance as done in [4], but with the fundamental difference that we will deliver anonymized data as output, not models.

In the above-described context, the specific goals of the internship are as follows:

- Experiment with GANs/VAEs using differential privacy for multiple datasets see https://github.com/SAP-samples/security-research-differentially-private-generative-models
- Design an architecture to optimize differential privacy budget consumption using transfer learning for generative model training
- Experiment with different transfer learning techniques to train generative models with differential privacy

Technologies/techniques involved are: Python, Tensorflow, SKLearn and Machine Learning in general

We expect that 70% of time will be dedicated to research activities, and 30% to development

REFERENCES

1. Shokri R, Stronati M, Song C, Shmatikov V. 2017 Membership inference attacks against machine learning models. In Proc. of the 2017 IEEE Symp. on Security and Privacy (SP), San Jose, CA, 22–24 May 2017, pp. 3–18. New York, NY: IEEE.
2. Pyrgelis A, Troncoso C, De Cristofaro E. 2018 Knock knock, who's there? Membership inference on aggregate location data. In Proc. of the Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, CA, 18–21 February 2018. Reston, VA: The Internet Society.
3. Lorenzo Frigerio, Anderson Santana de Oliveira, Laurent Gomez, Patrick Duverger: Differentially Private Generative Adversarial Networks for Time Series, Continuous, and Discrete Open Data. CoRR abs/1901.02477 (2019) http://arxiv.org/abs/1901.02477

4. Papernot, N., Abadi, M., Erlingsson, U., Goodfellow, I., & Talwar, K. (2016). Semi-supervised knowledge transfer for deep learning from private training data. arXiv preprint arXiv:1610.05755. https://arxiv.org/abs/1610.05755

CANDIDATE PROFILE

- University Level: Last year of MSc or less if the student has a good profile
- Good knowledge of the Python programming language
- Good knowledge of versioning control systems like GIT or SVN
- Good knowledge of deep learning, machine learning, transfer learning
- Interest in research work
- Fluency in English (working language)
- Good oral and written communication skills

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://jobs.sap.com/job/Mougins-Internship-Secure-Integration-of-Internet-of-Things-MF-Job-06/506679801/?locale=en_US

UPLOAD (all documents must be in English):

- Your CV
- Cover letter
- Any relevant documents