D-ITET – Professorship on Secure Machine Learning Systems

Profile

1. Context and focus of professorship

The goal of the Professorship is to secure Machine Learning (ML) systems with a focus on the entire ML software and hardware stack. ML systems are already highly complex, diverse, and heterogeneous, and these aspects will only intensify in the future as ML solutions are about to be integrated into many application domains. To give some inspiring examples, imagine a future where bank cards rely on specialized ML chips for authentication to improve security, a CPU that makes use of ML for optimizing its power or performance, or a security camera that aims to detect suspicious activity using built-in ML techniques. These systems will rely on specialized ML hardware/software stacks to implement application scenarios with an important security component. Unfortunately, the security of ML solutions has not been adequately covered by science even though they may be affected by a plenitude of vulnerabilities. Even worse, as we move towards new post-Moore architectures, there will likely be new system-level vulnerabilities that require special attention before such systems can be deployed in practice. This professorship aims to understand the attack surface of current and future ML systems by considering the entire software/hardware stack. This exploration will lead to new design principles for secure development of the entire ML software/hardware stack as well as guidelines for security testing of existing and future ML systems.

2. Research

The focus of the professorship is on machine learning security. The professorship will cover the following topics

- Analysis of safety issues and security vulnerabilities in ML systems considering the entire software/hardware stack.
- The professorship will handle a portfolio in ML systems and security. More precisely, the professorship will build up expertise in the secure and safe ML architectures, their hardware design and related software and algorithm concepts.
- The development of secure design principles as well as novel security testing techniques for future ML systems considering the entire software/hardware stack.

In the development of novel security solutions, the professorship will develop strong collaborations with existing faculty within D-ITET and it will work with industry towards solutions. The group headed by this professorship will be engaged in European initiatives and guarantee the exchange of knowledge at a European level.

3. Teaching

The position will cover the following topics in teaching

- Machine learning
- Machine learning security

- Machine learning hardware/software architectures and algorithms
- Testing procedures for reliable and trustworthy use of machine learning

The new colleague will contribute to teaching across these domains. She or he is expected to teach existing and new courses at the Bachelor and Master level. Finally, the new colleague will help us meet the increasing demand for Bachelor and Master theses.

4. Strategy

There is no denying that ML systems will be integrated in all aspects of our lives. Such systems will be highly complex, diverse, and heterogenous, creating a challenging environment for ensuring their security. Consequently, understanding and improving the security of ML systems, by focusing on their entire hardware/software stack, already has a significant importance to both science and society which will only increase as we explore new frontiers in ML and the emerging hardware that it will run on. Instead of reactively fixing security problems, we should seize the opportunity to design the ML systems of tomorrow with security in mind.

This professorship is of interest to D-ITET due to its interdisciplinary nature, it will have collaborations with D-INFK on software aspects and D-MAVT on possible future applications. We also envision strong collaborations with D-ITET professors that work in these domains, such as Prof. Wattenhofer, Prof. Vanbever on machine learning and its applications, Prof. Benini and Prof. Mutlu on ML hardware design and architecture, and Prof. Razavi on security. We also envision collaborations with D-INFK professors that work in ML, such as Prof. Vechev and Prof. Tramèr.

The professorship will further collaborate with and advise public bodies as well as local industry in matters related to ML safety aspects. One of the research goals and services towards the public would be to guarantee secure access to critical technologies that exploit and/or are based on ML algorithms.

This professorship from D-ITET will be unique at ETH Zurich given the focus on the security of the entire ML stack, considering both hardware and software.

Resources

1. Financial Aspects

The Professorship will be funded through the initiative from the canton of Zug and the National Test Institute for Cybersecurity (NTC).

2. Location

D-ITET can provide space at the OAT, Floor U 17-19. (Space of 102 m^2, 12 AP). The Professorship is expected to have a presence in the NTC as well, provided sufficient and suitable workingspace can be made available. Such presence would be helpful, e.g., for fostering local partnerships with industry and collaboration as well as the emergence of start-ups.