Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Beilage 1

D-INFK - PROFESSORSHIP IN AI FOR CYBERSECURITY

Profile

1. Context and focus of professorship

Modern cybersecurity challenges have grown exponentially in complexity and scale, making traditional manual security analysis increasingly insufficient. The rapid proliferation of sophisticated cyber threats, coupled with the expanding attack surface of interconnected systems, demands innovative approaches to cybersecurity. Artificial Intelligence and Machine Learning have emerged as powerful tools in this domain, offering unprecedented capabilities in threat detection, vulnerability discovery, and security automation.

Recent high-profile security incidents, such as the Log4Shell vulnerability, highlight the need for more advanced security analysis techniques. Traditional security tools and human analysts, while valuable, struggle to keep pace with the volume and sophistication of modern threats. AI-powered security solutions have demonstrated remarkable success in identifying patterns of attack, detecting anomalies, and even predicting potential vulnerabilities before they can be exploited.

The application of AI in cybersecurity spans multiple critical areas. Deep learning models have shown promise in malware detection and classification, often identifying novel variants that evade traditional signature-based approaches. Natural Language Processing techniques are being employed to analyze security reports, threat intelligence, and vulnerability descriptions, helping to automate the processing of security-relevant information. Machine learning algorithms are increasingly being used to identify potential vulnerabilities in source code and binaries, complementing and enhancing traditional static and dynamic analysis techniques.

The focus of this profile is therefore on advancing the state-of-the-art in AI-powered security analysis, including automated vulnerability discovery, threat detection, and security testing. This includes developing new AI architectures for security applications, improving the robustness of AI-based security tools, and creating novel approaches for combining AI with traditional security analysis techniques.

2. Research

The increasing complexity of cyber threats and the growing scale of software systems have made traditional security analysis methods insufficient on their own. Artificial Intelligence offers promising new approaches to enhance cybersecurity, but developing effective and reliable AI-based security solutions presents significant research challenges.

The focus of this professorship is to advance the state-of-the-art in AI-powered security analysis and defense mechanisms. The research spans various application domains including vulnerability discovery, threat intelligence, and automated security testing. Core research areas include:

- AI-powered vulnerability detection and exploitation
- Deep learning approaches for anomaly detection in system behavior
- Automated security testing using reinforcement learning
- AI-assisted reverse engineering and binary analysis

- Robust AI models for security applications
- Natural language processing for threat intelligence
- AI-powered fuzzing and penetration testing

The new professor will strengthen the bridge between artificial intelligence and information security, while also connecting to systems and software engineering. Their research will complement our existing strength in cybersecurity by introducing novel AI-based approaches to security analysis and defense. There are numerous opportunities for collaboration within the department (in particular with researchers working on machine learning, systems security, and software analysis) and beyond (for instance, with researchers working on robust AI and formal verification).

We expect the new professor to engage with both the academic community and industry partners. Collaboration opportunities exist with cybersecurity companies, not-for profit organizations such as the NTC, major tech firms developing AI security solutions, and financial institutions implementing AI-based security measures. The research should contribute to both the theoretical foundations of AI in security and practical applications that can improve the security of real-world systems.

3. Teaching

AI for cybersecurity represents a crucial intersection of machine learning, information security, and systems engineering. The new colleague will contribute to teaching across these domains, with a particular focus on the application of AI techniques to security challenges. They are expected to teach courses at the Bachelor and Master level, such as existing courses focusing on cybersecurity or a new course on AI approaches to security. Master courses in the proposed area will further strengthen the Secure and Reliable Systems track of the computer science master and also help expand the master’s in cybersecurity. Finally, the new colleague will help us meet the increasing demand for Bachelor’s and Master’s theses.

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

While the professorship and many of its activities will be located at Eth Zurich and within D-INFK, it is expected, that for certain activities a presence in Zug, e.g., in the NTC, provided sufficient and suitable working-space can be made available, will be helpful, e.g., for fostering local partnerships with industry and collaboration as well as the emergence of start-ups.