Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer
AISEC

Student Assistant (Wissenschaftliche Hilfskraft)/ Bachelor Thesis/ Master Thesis

SuKI Project[1]: IT Security and Artificial Intelligence

Motivation and Task Description

Increasing networking and digitization pose ever new challenges for IT security. On the one hand, artificial intelligence (AI) offers a wide range of opportunities. At the same time, it is becoming increasingly important to suitably quantify the security of AI. Often, questions about the sensible use of AI, the secure adaptation of algorithms, the privacy of data, suitable model protection or robustness cannot be answered satisfactorily. This is where the SuKI project, funded by the Bavarian state, comes in, to advance applied research at the interface between artificial intelligence and IT security.

Different aspects of the work may include, but are not limited to:

- **Adversarial machine learning** (e.g., image and audio domain, generation, detection),
- **Deepfakes** (e.g., audio deepfake, video deepfake),
- **Anomaly detection** (e.g., heterogeneous data sources, data encoding, human-in-the-loop),
- **Embedded AI** (e.g., federated learning, compact representations for neural networks),
- **Privacy-preserving machine learning** (e.g., model inversion, membership inference), and
- **AI-enhanced security tools** (e.g., penetration testing, fuzzing, side-channel analysis).

Please, state your topics of interest in your application.

Requirements

- Good general programming skills (ideally Python)
- Interest in deep learning and security research
- Ability to work self-directed and systematically
- Motivation and self-organization

Contact

Karla Markert
Telefon: +49 89 322-9986-136
E-Mail: karla.markert@aisec.fraunhofer.de

Dr. Konstantin Böttinger
Telefon: +49 89 322-9986-163
E-Mail: konstantin.boettinger@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Cognitive Security Technologies
Lichtenbergstraße 11, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de

Ausschreibungsdatum: 26. Februar 2021

[1] For more information, see `www.aisec.fraunhofer.de/suki`.