Chair of IT Security
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Student Assistant (m/f/)*

Testbed Creation for Exploitable Smart Building Devices

Smart buildings have a commonly known trade-off: residents can control, monitor, and automate their homes with connected ecosystems; However, the new living comfort is offset by threats to the privacy and security of residents. Built-in sensors, such as cameras and microphones, generate data flows that can be used to infer users' behavior and preferences. Smart home devices must be designed and developed securely to mitigate these threats and ensure privacy-preserving and trustworthy operation.

Task Description

Your objective is to build a smart building testbed capable of collecting confidential data from devices, which may be susceptible to exploitation. In the initial phase, smart building devices and sensors are connected to the multi-floor, multi-room network. Their confidentiality-sensitive data will be sent to edge devices over Zigbee, Thread, and Matter. These forward their traffic to a VM running on a central server. This VM will host a web server for data collection, enabling remote monitoring for Intrusion Detection and Privacy-Enhancing Technology research.

Requirements

- High motivation and ability to work independently on-premise at Fraunhofer AISEC.
- Knowledge about network protocols, databases, and any programming language (C, Python, Rust, Java, etc.) is required.
- Experience with smart home protocols, VMs, webservers, or CVEs is a plus

Contact

Please send your application with current CV and transcript of records to:

Veronique Ehmes
Product Protection and Industrial Security
Mail: veronique.ehmes@aisec.fraunhofer.de
Phone: +49 89 322 9986-1043

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Lichtenbergstr. 11, 85748 Garching near Munich

Publication Date: 21.11.2025