Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis

Hardware Supply Chain Security (AISEC)

Most customers put trust in their hardware vendors and the corresponding supply chain. No matter how well secured these customers' own infrastructures are, this trust has the potential to devolve the weaknesses of their vendors (and even the vendors' vendors etc.) into the customers' own environment, constituting a blind spot in their overall security architecture.
Proposals to address this multi-dimensional problem on the one hand include organizational measures as, for example, establishing Cyber Supply Chain Risk Management (C-SCRM) or demanding third-party certifications, which confirm conformance with standards such as the ISA/IEC 62443 series. On the other hand, technology-based approaches as, for example, physical unclonable functions or IDevID certificates can also help to decrease the amount of trust which has to be put into the hardware supply chain.

Topic
The overall goal of this guided research is to compile a comprehensive overview of the hardware supply chain security landscape including challenges and potential solutions/countermeasures. The focus should lie on but not solely be limited to industrial automation and control systems (IACS).
The first part is to investigate both real-world incidents and academic approaches exploiting the hardware supply chain. Based on this preliminary research and reasoning, a holistic paradigm of trust relationships and corresponding problems in the hardware supply chain has to be derived and consolidated.
In the second part, suitable countermeasures have to be investigated and mapped to this paradigm. These countermeasures should in turn be categorized based on their maturity (ready-to-use, academic PoC, proposal etc.).

Prerequisites

- Self-initiative and the ability to work in a self-directed way
- Knowledge in the field of IT/IACS security
- First experiences with hardware security would be ideal

Please attach a current grade sheet and a short CV to your application.

Contact

Michael Heinl
Nikolai Puch
Phone: +49 89 322-9986-125
Phone: +49 89 322-9986-142
E-mail: michael.heinl@aisec.fraunhofer.de
E-mail: nikolai.puch@aisec.fraunhofer.de
Fraunhofer Research Institute for Applied and Integrated Security AISEC
Department Product Protection and Industrial Security Lichtenbergstraße 11, 85748 Garching near Munich, Germany https://www.aisec.fraunhofer.de

Advisors

Georg Sigl
Michael Heinl und Nikolai Puch (Fraunhofer AISEC)