Tamper-Resistant Envelope: Prototyping and Attacks

Tamper-resistant envelopes based on Physical Unclonable Functions (PUFs) are used to cover and protect embedded systems from unwanted manipulation by an attacker. Whether a tampering event occurred is determined by measuring the capacitance of electrodes in the envelope. This measurement process was integrated into a custom ASIC. The future tasks are to integrate the ASIC into a prototype and to perform attacks on the envelope.

Task Description
In our research group we need support in terms of:

- Prototype Hardware Design
- Driver Implementation for ASIC Communication
- Non-Invasive Attacks on the Envelope

Prerequisites
Depending on the actual work carried out:

- Background in Circuit/PCB Design (incl. Soldering)
- Experience with C and Embedded Devices
- Creativity and Independent Work Style
- Interest in IT Security

Contact
Kathrin Garb, M.Sc.
Fraunhofer Institute AISEC
Physical Security Technologies Group
Lichtenbergstraße 11, 85748 Garching (near Munich)
email: kathrin.garb@aisec.fraunhofer.de

Advisors
Georg Sigl
Kathrin Garb (Fraunhofer AISEC)