Thema:

Manipulationsresistente Hardware für mobile Computer

Seminar „Mobile Business“, WiSe 2010/11

Betreuer: Michael Decker (m.decker(at)kit.edu)

Aufgabenstellung:

Manipulationsresistente Hardware (Tamperproof Hardware, Hardware Security Module) sind spezielle Hardware-Komponenten, die auch bei direkten physischen Manipulationen bestimmte Sicherheitsziele garantieren sollen. Solche Hardware-Komponenten kommen etwa dann zum Einsatz, wenn bestimmte geheime Informationen etwa beim Diebstahl des Geräts vor dem Angreifer geschützt werden soll.

Im Rahmen des Themas soll vorgestellt werden, welche physischen Angriffe auf Hardware-Komponenten es gibt (z.B. Auslesen unter Elektronenmikroskop, Seitenkanalangriffe, Betrieb mit unzulässigen Stromspannungen) und mit welchen Maßnahmen die Hardware hiergegen geschützt werden kann (z.B. Selbstzerstörungsmechanismus, Einlegen in Bohrschutzmembran, Druck-Temperatursensoren, spezielles Design der Leiterbahnen). Es soll insbesondere dabei auch auf für mobile Anwendungen geeignete manipulationsresistente Hardware-Komponenten eingegangen werden, wobei auch entsprechende Anwendungsszenarien von Interesse sind.

Literatur:

- Kömmerling, Kuhn: Design Principles for Tamper-Resistant Smartcard Processors. Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illionois, 1999, 9-20.
- Fox: Hardware Security Module (HSM). Datenschutz & Datensicherheit (DuD), 9/2009, 564.
- Bond: Understanding Security APIs. Dissertation, University of Cambridge, U.K., 2004. (v.a. Kapitel 6)