Thema:

„Smartcards für mobile Sicherheit“

Seminar „Mobile Business“, WiSe 2010/10

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

Aufgabenstellung:

In Rahmen des Themas sollen kommerzielle Smartcard-Produkte mit Sicherheitsfunktionen untersucht werden, die speziell für mobile Computer (z.B. Smartphones, Notebooks) entwickelt sind (z.B. in Bauform von (micro)SD-Karten, Express Card oder SIM-Karten). Solche Smartcards bietet etwas Verschlüsselungsfunktionen oder können Daten sicher speichern („Tresor-Funktion“). Die Sicherheitsfunktionen sollten aufrechterhalten werden können, auch wenn sich die Smartcard im direkten Besitz des Angreifers befindet, der diese etwa mit spezieller Laborausrüstung analysieren kann.

Relevante Aspekte:

- Gibt es spezielle Programmier-Schnittstellen, um die Sicherheitsfunktionen anzusprechen?
- Welche Algorithmen/Funktionen bieten die Karten?
- Wird genannt, welche speziellen Maßnahmen die Manipulationsresistenz gewährleisten sollen (z.B. spezielles Layout der Leiterbahnen)?

Einstiegsliteratur / Links:

- Kömmerling, Kuhn: Design Principles for Tamper-Resistant Smartcard Processors. Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illionois, 1999, 9-20.
- Produkte der Firma Certgate: http://www.certgate.com/index.php?id=16
- Produkte der Firma WiBu: http://wibu.de/download_data.php
- Produkte der Firma Giesecke & Devrient: http://www.gi-de.com/portal/page?_pageid=42,95141&_dad=portal&_schema=PORTAL