Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

Fachbereich Ingenieurwissenschaften
Fachgebiet Informationstechnik & Telekommunikation
Prof. Dr.-Ing. Karl Heinrich Hofmann

Vortragsankündigung

Am **Freitag, dem 14. Dezember 2018, 14^{00} Uhr**, findet im M-Lab (Raum 405, 4. Stock, Gebäude A1 Nord) folgender Vortrag statt.

Angriffe auf IT Sicherheitscontroller

Dr. Patrick Bödeker

Leiter der Abteilung Hardware Evaluation,
TÜV Informationstechnik GmbH, IT Security, Essen

Es vergeht kaum ein Tag, an dem nicht über neue Angriffe auf IT Systeme berichtet wird. Mit zunehmender Vernetzung verschiedenster Systeme von der Heimanwendung bis hin zu industriellen Steuerungssystemen wird der Einsatz von Sicherheitskomponenten immer wichtiger. So werden zum Schutz sensibler Daten z.B. in Kreditkarten, in hoheitlichen Dokumenten, in der Gesundheitskarte oder im Smartphone schon seit langem Hardware-Sicherheitsmodule und Chipkarten eingesetzt. Neben der reinen Hardwaresicherheit ist dabei auch die sichere Implementierung von kryptografischen Algorithmen (z.B. RSA, elliptischen Kurven) von zentraler Bedeutung. Der Anwendungsbereich solcher Sicherheitsanker wird immer größer werden und nicht auf Hochsicherheitsanwendung beschränkt bleiben.

Die Rahmenbedingungen für die Prüf- und Messverfahren werden entweder durch internationale Normen und Spezifikationen wie z.B. Common Criteria, FIPS PUB 140-2 sowie Spezifikationen der internationalen Kreditwirtschaft und Zahlungsdienstleister (DK, EMVCo) definiert. Eine umfangreiche Sicherheitsanalyse beinhaltet eine Überprüfung des gesamten Lebenszyklus des Produktes. Dies schließt die Sicherheit der Entwicklungs- und Produktionsumgebung, eine detaillierten Designprüfung (bis auf Quellcode- und Layoutebene) und umfangreiche Penetrationstest im Hardware-Testlabor ein.

Der Vortrag gibt eine Übersicht über Angriffsmethoden auf IT Sicherheitscontroller und einen Einblick in das Hardware Sicherheitslabor der TÜViT. Typische Angriffsmethoden wie Seitenkanalanalyse (Power Analysis: SPA, DPA, Electromagnetic Emanation Analysis: SEMA, DEMA) und Fehlerinduktion (Laser Fault Injection - LFI, Voltage and frequency manipulation, Differential Fault Analysis - DFA) werden vorgestellt.

Dr. Patrick Bödeker hat seine Promotion auf dem Gebiet der experimentellen Festkörperphysik an der Ruhr Universität Bochum erlangt. Er ist seit 1997 bei der TÜV Informationstechnik GmbH beschäftigt und leitet die Abteilung Hardware Evaluationen. Er ist verantwortlich für das HW-Labor Sicherheitslabor der TÜViT und die Prüfung von Hardware Sicherheitsprodukten (Sicherheitscontroller, Hardware-Sicherheitsmodule, etc), dem elektronischen Zahlungsverkehr und der Mobile Security.

Die Dauer der Präsentation beträgt ca. 60 Minuten plus anschließende Diskussionsrunde. Die Veranstaltung ist öffentlich, und alle Interessenten sind dazu herzlich eingeladen.

Hochschule RheinMain, Am Brückweg 26, D-65428 Rüsselsheim
URL: http://www.hs-rm.de