CASCADE research group

CONSTRUCTIVE ATTACKS | SIDE CHANNEL ANALYSIS | SECURE DESIGN

http://cascade.cased.de

TECHNISCHE UNIVERSITÄT DARMSTADT

Dozent: Prof. Dr. Werner Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI) / TU Darmstadt / CASED

e-Mail: werner.schindler@cased.de

Blockveranstaltung SS 2010

Seitenkanalangriffe und Fault Attacken gegen IT-Systeme

INHALT DER VORLESUNG:

Mathematik: Modellierung von Seitenkanalinformationen durch stochastische Prozesse und deren Analyse, statistische Entscheidungstheorie, multivariate Statistik und elementare Zahlentheorie

Kryptographie und IT-Sicherheit: Seitenkanalangriffe (Laufzeitangriffe, Powerangriffe, Cachebasierte Angriffe) und Fault Attacken

Vorlesungsbegleitende Übungen vertiefen und ergänzen den Stoff und illustrieren ihn durch praktische Beispiele.

FORM DER LEHRVERANSTALTUNG: V2 + Ü1

TERMINE:

Der erste Vorlesungsblock findet am

Freitag, den 23. April 2010, 18:30 - 20:00 Uhr
Samstag, den 24. April 2010, 10:00 - 11:30 Uhr
Samstag, den 24. April 2010, 13:00 - 14:30 Uhr

im Mathematikgebäude der TU Darmstadt in der Schlossgartenstr. 7, Raum S 215 / 51 statt.

Die weiteren Vorlesungstermine und die Übungstermine werden im ersten Vorlesungsblock mit den Teilnehmern abgestimmt.