



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Ansprechpartner:

Dipl.-Inform. Michael Kasper
michael.kasper@sit.fraunhofer.de
06151 869-60012

Fraunhofer-Institut
Sichere Informationstechnologie
Rheinstraße 75
64295 Darmstadt

Prof. Dr. Claudia Eckert
Fachbereich Informatik
FG Sicherheit in der
Informationstechnik
Hochschulstr. 10
64289 Darmstadt
Telefon +49 (0) 61 51/16-6591
Telefax +49 (0) 61 51/16-3514

Fraunhofer Institut
Sichere Informationstechnologie SIT
Institutsleitung
Prof. Dr. Claudia Eckert

Rheinstraße 75
64295 Darmstadt

E-Mail: eckert@sit.fraunhofer.de
<http://www.sit.fraunhofer.de>

Ausschreibung eines Praktikums (6CP)

Thema: „OpenMTP“ - Umsetzung einer Sicherheitsarchitektur für mobile Endgeräte

Die angewandte Forschung des Fraunhofer-Institut SIT in Darmstadt beschäftigt sich intensiv mit Anwendungsgebieten im Bereich Trusted Computing. Hierfür suchen wir motivierte Studenten, die sich für Sicherheitslösungen in zukünftigen mobilen Endgeräten, Virtualisierung und sichere Betriebssysteme interessieren.

Hintergrund: Im Juni 2007 veröffentlichte die Trusted Computing Group (TCG) eine umfassende Referenzarchitektur zur Modellierung von Sicherheit und Vertrauen auf Basis des Mobile Trusted Module (MTM), die mobile Endgeräte für kommerzielle Dienstleistungen sicherer machen soll.

In diesem Sicherheitskonzept wird eine Mobile Trusted Platform (MTP) als eine Menge von manipulations-geschützten und vertrauenswürdigen Ausführungsumgebungen (Trusted Engines) spezifiziert. Dabei stellt jede Umgebung einen streng isolierten und einem bestimmten Interessensvertreter (z.B. Gerätehersteller, MNO oder Eigentümer) zugeordneten Bereich dar, in dem verschiedene Software-Funktionalitäten als vertrauenswürdige und/oder normale Dienste implementiert werden können.

Ziel des Praktikums: Im Rahmen dieser Arbeit soll die prototypische Implementierung der TCG MPWG Reference Architecture [1] auf Basis eines vertrauenswürdigen Betriebssystems untersucht und durchgeführt werden. Dabei werden mehrere Trusted Engines als isolierte Linux-Instanzen parallel ausgeführt und ausgewählte Dienste und notwendige Roots-of-Trust realisiert. Ferner soll ein bereits existierender Open-Source MTM-Emulator für diesen Zweck angepasst und erweitert werden.

Voraussetzungen: Erforderlich sind Vorkenntnisse im Bereich Betriebssysteme, etwa aus einschlägigen Vorlesungen und/oder eigener praktischer Anwendung. Für die Implementierung sind gute Programmierkenntnisse in C/C++ notwendig. Vorkenntnisse im Bereich Trusted Computing sind hilfreich, können aber auch während des Praktikums angeeignet und vertieft werden.

Das Thema kann in Gruppenarbeit von maximal vier Studenten bearbeitet werden. Eine eigenständige, zielorientierte Arbeitsweise wird erwartet.

Das Praktikum wird für das **IT-Sicherheits-Zertifikat** anerkannt.

Beginn: ab sofort

Weitere Informationen: erhalten Sie bei

Dipl.-Inform. Michael Kasper

(michael.kasper@sit.fraunhofer.de, 06151 869-60012)

Dipl.-Inform. Nicolai Kuntze

(nicolai.kuntze@sit.fraunhofer.de, 06151 869-276)

Dr. Andreas U. Schmidt

(andreas.schmidt@sit.fraunhofer.de, 06151 869-60227)

Hintergrundmaterial:

Einstieg:

Vorlesung ‚Trusted Computing‘ im SS07. Folien unter

<http://www.sec.informatik.tu-darmstadt.de/index.php?lang=de&page=pages/lehre/SS07/tc/material.html>

Vertiefung:

TCG MPWG Reference Architecture, Specification version 1.0

Revision 1, Trusted Computing Group,

<https://www.trustedcomputinggroup.org/specs/mobilephone/>