



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Contact:

Fraunhofer-Institute
Secure Information Technology
Rheinstraße 75
64295 Darmstadt

Dr. Andreas U. Schmidt

Andreas.U.Schmidt@sit.fraunhofer.de

Tel. 06151 – 869 60 227

Nicolai Kuntze

Nicolai.Kuntze@sit.fraunhofer.de

Tel. 06151 – 869 60 054

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>

Diploma/Master Thesis

SUBJECT: Securing Digital Evidence

Background and Goal: Evidence like measurements, photos, or documents in its broadest sense includes anything that is used to determine or demonstrate the truth of an assertion as it is needed for example in court. Various kinds of evidence are known mostly bound to a physical representation. Digital evidence like a photo or other measured values are here different as they are only existent in a binary representation were modifications and tampering is hard to detect. Therefore this kind of evidence requires appropriate additional methods to show and preserve their significance over a long period of time.

If the evidence is created in an automated process, for instance in the case of speed monitoring, it may be required to collect also data showing the state of the device used to create the evidence. These data testify that the device was during the measurement process in a well defined state and operated according to the specification. During a subsequent verification the monitored data together with the securing data shall prove that a certain event happened at the specified time and location and that the information was not tampered during or before the process of securing took place.

This thesis will use the technological base offered by Trusted Computing to achieve

- A concept for the creation of digital evidence in automated processes approaching the challenge of integrity protection of digital evidence.
- The application of digital certificates in combination with Trusted Computing concepts like system attestation
- a demonstration application implementing the developed concepts

Prerequisites: Good knowledge in IT security and interest in Trusted Computing. English writing skills are required as well as knowledge in C++ and Java.

Start: Immediately