Contact:
Fraunhofer-Institute
Secure Information Technology
Rheinstraße 75
64295 Darmstadt

Dr. Andreas U. Schmidt
Andreas.Schmidt@sit.fraunhofer.de
Tel. 06151 – 869 60 227

Nicolai Kuntze
Nicolai.Kuntze@sit.fraunhofer.de
Tel. 06151 – 869 60 054

TECHNISCHE UNIVERSITÄT 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

Diploma/Master Thesis

SUBJECT: Trusted Computing Security for Web-Browsers

Background and Goal: Trusted Computing (TC) as defined by the Trusted Computing Group is sometimes seen as a protection technology centred on protection of media (DRM). But this upcoming technology has many facets which applied information security can benefit from. Seen as a platform-neutral security infrastructure, TC offers ways to establish trust between entities that are otherwise separated by technical boundaries, e.g., different access technologies and access control structures. Trusted Computing also offers to users of PCs attractive features and an easily accessible infrastructure to protect their secret data on their own computing platforms. Simplest examples are encrypted file systems using TPM-protected keys.

Web-Browsers, on the other hand, use a software token approach to store, manage, and protect user credentials such as certificates, cookies, browser history, etc. The thesis shall enhance Web Browser security by TPM protection methods. Main goals are

- Development of a security architecture founded on TPM functionality for a common browser on standard (e.g. open source) platforms. Functionality comprises
  - Optimal leveraging of TPM Key hierarchy
  - Fine granular differentiation of protection methods for different secrets
  - Concepts for backup / re-storage
  - Concepts for migration between platforms
- Development of a Browser-based user Interface (e.g. a Browser plugin) to manage TPM protection of Browser secrets. TPM facilities will be accessed via open source standard APIs such as jTSS or tpm4java.
- Demonstrate the foregoing results

Prerequisites: Good knowledge of Web Browser security. Knowledge in cryptography. Elements of Trusted Computing. Fluent in Java and knowledge of contemporary Web-application technology.

Start: Immediately