Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Andreas Fuchs
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-228
Fax 06151 869-224
andreas.fuchs@sit.fraunhofer.de
www.sit.fraunhofer.de

SOFTWARE-PLATTFORM FÜR TPM 2.0

SICHERHEIT FÜR AUTOMOTIVE-IT

Viele Produktinnovationen im Auto basieren auf IT-Systemen und deren Internetanbindung. Doch die zunehmende Vernetzung birgt auch neue Angriffsmöglichkeiten. Basierend auf einem TPM 2.0 hat das Fraunhofer SIT eine Software-Plattform entwickelt, mit der sichere Steuergeräte entwickelt werden können.

Die Kombination von IT mit der physikalischen Welt spielt in vielen Branchen eine immer größere Rolle. Beispiel Auto: Das vormals geschlossene System Auto ist mit über 100 eingebetteten Steuergeräten, Sensoren und anderen Mini-Computern ausgestattet, die untereinander und mit den Backendsystemen der Hersteller kommunizieren oder mit dem Internet verbunden sind. So ergeben sich einerseits vielfältige neue Anwendungsmöglichkeiten. Andererseits sind Fahrzeuge dadurch vielen neuen Gefahren ausgesetzt. Hacker spionieren sowohl persönliche wie herstellerspezifische Daten aus, Autodiebe überlisten die Wegfahrsperre. Wird das Kartenmaterial im Navigationssystem manipuliert, hat das im schlimmsten Fall Auswirkungen auf Leib und Leben der Fahrzeuginsassen.

Mehr Sicherheit

In Anbetracht der Vielzahl entdeckter Schwachstellen in den vergangenen Jahren bedarf es neuer Konzepte zur Sicherung der Integrität verbauter Steuergeräte. Dafür hat das Fraunhofer SIT eine Software-Plattform auf Basis herstellerunabhängiger offener Standards entwickelt. Die Lösung setzt auf einem Hardware-Sicherheits-Modul (HSM) auf, dem Trusted Platform Module (TPM) in der Version 2.0. Der Software-Anteil der Lösung kommuniziert dabei mit dem TPM, welcher als Vertrauensanker und Speicher kryptografischer Schlüssel dient. Diese werden nur freigegeben, wenn die Geräte in einwandfreiem Zustand sind. Wird ein Angriff registriert, etwa eine Manipulation der Bremsen, kann das Motorsteuergerät zum Schutz der Insassen den Start des Fahrzeugs verweigern. Diese Funktionen lassen sich nutzen, um bei Firmware-Updates zu prüfen, ob sie aus einer vertrauenswürdigen Quelle stammen, und andernfalls den Zugriff auf kryptografisch gesicherte Speicher zu unterbinden. Dieser Mechanismus lässt sich so erweitern, dass das Wieder-Einspielen veralteter und womöglich verwundbarer Original-Firmwareversionen verhindert wird. Auch der Einbau gefälschter Ersatzteile kann mit diesem Ansatz erkannt und verhindert werden, da die im TPM hinterlegten Schlüssel ein Gerät als Originalteil identifizieren und nicht auslesbar oder kopierbar sind. So werden Hersteller nicht nur vor Produktpiraterie geschützt, auch Fahrzeughalter laufen nicht Gefahr, durch minderwertige Teile einen Unfall zu verursachen.

Das Fraunhofer SIT bietet den Prototypen zur Lizenzierung an. Darüber hinaus bietet das Fraunhofer SIT weitere Entwicklungen von Lösungen zur Geräteabsicherung aufbauend auf TPM 2.0.

Das bietet die Software-Plattform für TPM 2.0

- Firmware-Manipulationen werden erkannt und verhindert
- Schutz von privaten und herstellerspezifischen Daten
- Schutz vor Produktpiraterie
- Leichte Realisierung weiterer Sicherheitsprotokolle
- Nur geringe Speicher- und Rechenkapazität notwendig
- Unterstützung des Entwicklungsprozesses durch Hard- und Software-Simulatoren