Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

TRUSTED COMPUTING FÜR INDUSTRIE 4.0

SICHERHEIT FÜR EINGEBETTETE SYSTEME IN INDUSTRIELLEN NETZEN

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

Industrielle Anlagen sowie Produktions- und Handelsprozesse werden zunehmend vernetzt und digitalisiert. In dieser offenen, vernetzten Industrie spielt jedes Gerät eine wichtige Rolle für die Sicherheit des Gesamtsystems. Gleichzeitig stellt damit auch jedes in ein industrielles Netz eingebettetes Gerät ein attraktives Ziel für Angreifer dar. Mit Methoden des Trusted Computing lassen sich Hardware-Komponenten eindeutig identifizieren und ein vertrauenswürdiger Systemzustand (Integrität) sicherstellen. Das Fraunhofer-Institut für Sichere Informationstechnologie SIT bietet Beratung, Konzepte und Lösungen im Bereich Trusted Computing, um Maschinen abzusichern und industrielle Netze zu schützen.

Vor der Digitalisierung und Vernetzung industrieller Produktionsanlagen mit dem Internet waren industrielle Netze in sich geschlossen, jede Maschine, jedes Gerät konnte vor Ort eindeutig identifiziert werden. Mit der Öffnung von Produktionsanlagen ins Internet, der Fernwartung von Anlagen oder dem Einspielen von Updates über Remote-Zugriff braucht man mehr, um Manipulationen auszuschließen: Eine sichere Industrie 4.0 funktioniert nur, wenn jede Maschine, jedes Stück Hardware, jedes Gerät eine eigene, nicht klonbare Identität hat, die auch die Integrität der laufenden Firmware umfasst. Dies gilt sowohl für große Produktionsanlagen als auch für kritische Infrastrukturen. Der Computerwurm Stuxnet etwa hatte die Software auf Geräten innerhalb eines industriellen Netzes unerkannt verändert und damit Manipulationen ermöglicht. Mit Methoden des Trusted Computing kann ein ähnlicher Angriff wirkungsvoll verhindert werden.

Das Fraunhofer SIT entwickelt auf Trusted Computing basierende Technologien und Lösungen für Hersteller, um Datenvertraulichkeit und Datenintegrität in eingebetteten Systemen sicherzustellen. Darüber hinaus konzipiert das Fraunhofer SIT vertrauenswürdige Anwendungen und Systemarchitekturen auf Basis von Hardware-Vertrauensankern. Netzbetreiber und Zuliefererbetriebe können sich von den Trusted Computing-Experten des Fraunhofer SIT technisch beraten lassen.

Unser Angebot

Beratung, Konzeption und Prototypisierung

- Technische Beratung, Erstellung von Konzepten und Analysen
- Machbarkeitsstudien und prototypische Implementierungen
- Unterstützung bei Umsetzung von Trusted Computing-Projekten

Fraunhofer SIT TPM Software Stack 2.0

- Middleware zur Nutzung aller TPM 2.0-Funktionalitäten
- Leichte Realisierung von TPM-basierten Sicherheitslösungen und -protokollen
- Konfigurierbarkeit für eingebettete Geräte bspw. zur Reduzierung der Speicheranforderungen

Fraunhofer SIT TPM/TSS 2.0 Development Tools

- Unterstützung des Entwicklungsprozesses durch Hard- und Software-Simulatoren
- Rapid Prototyping Tools zur schnellen Erstellung von Machbarkeitsstudien
- Ausgiebiges und konfigurierbares Logging- und Debug-Framework