Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

TRUSTED CORE NETWORK

HARDWAREBASIERTE SICHERHEIT FÜR INDUSTRIELLE IT-NETZE

Fraunhofer-Institut für Sichere Informationstechnologie

Kontakt:
Andreas Fuchs
Rheinstraße 75
64295 Darmstadt

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

Um Produktions-, Steuerungs- und Wartungsprozesse zu verbessern, vernetzen Unternehmen ihre industriellen Umgebungen mit Büro-IT und Internet. Dadurch steigt die Gefahr, dass es zu Störungen in den Betriebsabläufen kommt oder Angreifer Industrieanlagen und Maschinen gezielt manipulieren oder sabotieren. Um dem entgegenzuwirken, hat Fraunhofer SIT eine hardwarebasierte Lösung zur Absicherung industrieller Netzwerke entwickelt. Sie erfüllt die Industrieanforderungen hinsichtlich Echtzeitperformanz, Verfügbarkeit und IT-Sicherheitsniveau und lässt sich einfach und kostengünstig in bestehende industrielle IT-Netze integrieren.

Für IT-Infrastrukturen in Produktionsanlagen oder in der Automatisierung gelten besondere Anforderungen. Insbesondere die Verfügbarkeit der Systeme und die Einhaltung von Echtzeitanforderungen an die Kommunikationstechnologie sind für Produktions- und Steuerungsprozesse essenziell, um Produktionsausfälle zu vermeiden. Bislang waren industrielle Umgebungen und ihre IT-Netze von Büro-IT und Internet getrennt. Zur Verbesserung von Produktionsdurchfluss und Reduzierung von Lagerbeständen schafft die Industrie jetzt jedoch mehr und mehr Verbindungen zwischen verschiedenartigen IT-Netzen, darunter auch Netze außerhalb der Kontrolle des produzierenden Unternehmens.

Standardlösungen zur Netzabsicherung sind Firewall und Virtuelle Private Netze (VPN). Diese Lösungsansätze stammen aus der IT-Welt, werden den besonderen Anforderungen industrieller Umgebungen jedoch oft nicht gerecht, denn sie verzögern teilweise die prozessrelevante Kommunikation und sorgen mitunter für erhöhte Komplexität. Darüber hinaus haben industrielle Netzwerke andere Anforderungen an den Schutz ihrer Grenzen bzw. Perimeter. Beispiel Fernwartung von Produktionsanlagen: Hier müssen zwingend Dienstleister beteiligt werden, was zu einer komplexen Bedrohungssituation führt. Außerdem gewährleisten herkömmliche IT-Sicherheitsarchitekturen nicht die für Industrieanlagen notwendige Hochverfügbarkeit, denn die Sicherheitsanforderungen an Office IT sind nicht vergleichbar mit denen in der Produktion und Automatisierung: Wenn Steuerungssysteme betroffen sind, können Manipulationen physischen Schaden anrichten und sogar für Mensch und Umwelt gefährlich werden. Auch Themen wie etwa die Gewährleistung für geleaste Maschinen müssen berücksichtigt werden. Deshalb hat Fraunhofer SIT zusammen mit seinen Partnern eine neuartige Lösung entwickelt, welche die Netzknoten als Basiskomponenten sichert und so eine vertrauenswürdige Basis für den Aufbau von sicheren Informations- und Kommunikationsinfrastrukturen ermöglicht.

Hardwarebasierter Vertrauensaufbau

Das Trusted Core Network (TCN) des Fraunhofer SIT ist in der Lage, die Identität von Netzknoten zu prüfen und einen gewünschten Zustand der Netzknoten zu gewährleisten: Dazu nutzt das TCN eine verteilte/redundante Kontrolle der Netzknoten, die peer-to-peer Identität und Zustand der benachbarten Knoten prüft. Durch ein Trusted Network Discovery-Protokoll werden alle aktiven Geräte in der direkten Umgebung gefunden. Unter Verwendung des Trusted Platform Module (TPM) identifiziert das System den Knoten und vergleicht den Ist-Zustand mit dem geforderten Soll-

Zustand. So werden Manipulationen schnell erkannt, Warnungen direkt an ein zentrales Monitoring weitergegeben und die Ausbreitung von Angriffen und Malware unterbunden. Neben der Geräte-Identität prüft das Trusted Core Network die installierte und zur Ausführung geladene Software sowie die Konfigurationsdaten. Dadurch können Reaktionen dann gezielt eingeleitet werden, sodass trotz Manipulation oder erfolgreicher Angriffe auf einzelne Komponenten wichtige Funktionen aufrecht erhalten werden (Resilienz).

Zero-Touch Configuration

Wird ein neues Gerät in ein Trusted Core Network integriert, muss es entsprechend konfiguriert werden. Um ein effizientes Management zu ermöglichen, hat Fraunhofer SIT ein Protokoll zur Zero Touch Configuration entwickelt, das ebenfalls auf den Sicherheitsfunktionen des TPM basiert. Die Registrierung der Geräte benötigt lediglich eine eindeutige Gerätekennung, z. B. einen per QR-Code automatisch eingelesenen Fingerprint eines kryptographischen Schlüssels. In der Produktion des Geräts muss keinerlei kundenspezifische Information eingebracht werden, sodass die typischen Mehrkosten für komplexe Sicherheitslösungen, wie zum Beispiel für Public Key-Infrastrukturen,vermieden werden. Schließt der Techniker das Gerät an, laufen die Konfiguration, Registrierung usw. vollautomatisch. Keine USB-Sticks, kein Laptop, kein Nutzerinterface am Gerät sind zur Konfiguration nötig. Einer physikalischen Interaktion bedarf es lediglich im Fehlerfall

Implementierung

Das Konzept des Trusted Core Network wurde von Fraunhofer SIT in Zusammenarbeit mit Industriepartnern für zwei Einsatzumgebungen prototypisch umgesetzt. Für Industrienetze werden handelsübliche Hirschmann Eagle-Router verwendet, die durch TPMs am I²C Bus erweitert wurden. Diese Router prüfen alle Geräte in direkter Nachbarschaft und berichten die Ergebnisse an einen IF-MAP Server, über den die Informationen zum aktuellen Zustand des Netzes visualisiert werden. Das Trusted Core Network wurde im Rahmen des BMBF-Projektes ANSII entwickelt, um eine sichere Grundlage für die Erkennung von Anomalien in industriellen Netzen zu gewährleisten.

Vertrauenswürdige kabellose Netze

Gerade in weitläufigen Netzen stellt die kabelgebundene oder Access Point-zentrierte Kommunikation oft ein Problem dar. Daher werden in solchen Umgebungen verstärkt sogenannte Mobile Ad-Hoc-Netze (MANET) verwendet. In einem MANET übernehmen alle Geräte im Netz die Aufgabe eines Netzknotens und geben Routing-Informationen an andere Knoten weiter. Das am Fraunhofer SIT entwickelte TrustMANET wendet das Konzept des Trusted Core Network im Bereich der mobilen ad-hoc Netze an. Die gegenseitige Prüfung der Netzknoten wird durchgeführt, bevor ein Knoten in das Netz aufgenommen wird, und muss danach regelmäßig wiederholt werden. Damit erschwert man auch die Ausbreitung von Angriffen im Netz. Die Entwicklung von TrustMANET wurde teilweise von der Europäischen Kommission im Projekt SecFutur finanziert.

Angebot

- Entwicklung von Sicherheitsarchitekturen für kritische ITK in Produktion, Automatisierung und hochintegrierten Systemen
- Integration existierender Sicherheitsmechanismen
- Entwicklung neuer Protokolle und Sicherheitsfunktionen
- Unterstützung bei der Entwicklung neuer Produkte
- Erweiterung existierender Produktlinien mit hardwarebasierter Sicherheit
- Beratung zu hardwarebasierter Sicherheit
- Bewertung von Sicherheitsarchitekturen

Projektpartner:

Förderpartner:

Project SecFutur has received funding from the European Union's Seventh Framework Prgramme for research, technological development and demonstration under grant agreement no 256668.

Das Projekt ANSII wurde vom Bundesministerium für Bildung und Forschung gefördert.

GEFÖRDERT VOM