Schutz von Industrie4.0-Plattformen

Trusted Core Netzwerke in dezentralen Versorgungsnetzen

Kai-Oliver Detken

Heutige Industrieanlagen sind mit steigender Automatisierung durch dezentrale, vernetzte Rechner-, Mess-, Steuer- und Regelsysteme gekennzeichnet. Zunehmend finden sie auch in Bereichen der Kritischen Infrastrukturen Anwendung, wo ein Risiko von Ausfällen problematische Folgen haben kann. Eine erfolgreiche Absicherung von Industriesteuerungen setzt allerdings voraus, dass sich alle Kommunikationspartner unter Nutzung von Vertrauensankern gegenseitig identifizieren und authentisieren. Daher entwickelt das Forschungsprojekt TRUSTnet als Lösung eine Gesamtplattform für Industrie 4.0 auf Basis des Trusted Platform Modules (TPM), die garantierte Sicherheitseigenschaften bietet: ein sogenanntes Trusted Core Network (TCN) wird aufgebaut. Wir sehen uns die Funktionsweise und die sich daraus ergebenden Vorteile genauer an.

Die Basis einer sicheren Informations- und Kommunikationsinfrastruktur ist die Sicherstellung der Identität und Integrität aller beteiligten, kritischen Systeme unter Nutzung eines Trusted Core Networks (Foto: Panumas Nikhomkhai, pixabay)

Klassischerweise wurden Prozesssteuerungssysteme in Industrieanlagen meist als getrennte Netze betrieben. Im Rahmen von Industrie 4.0 wird aber die Vernetzung über das Internet immer wichtiger. Dies führt zu neuen Bedrohungen, die bei der ursprünglichen Entwicklung dieser Systeme nicht vorgesehen waren. Durch diesen Trend haben sich verschiedene Bedrohungsszenarien etabliert. Das BSI hat hierzu im Rahmen der Allianz für Cyber-Sicherheit eine Top-10-Liste zu den Bedrohungen für Industrial Control Systems (ICS) herausgegeben, die kontinuierlich aktualisiert wird. Aktuell lassen sich die folgenden 10 kritischsten Bedrohungen nennen:

1. Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme
2. Infektion mit Schadsoftware über Internet und Intranet
3. Menschliches Fehlverhalten und Sabotage
4. Kompromittierung von Extranet und Cloud-Komponenten
5. Social Engineering und Phishing
6. (D)DoS Angriffe
7. Internet-verbundene Steuerungskomponenten
8. Einbruch über Fernwartungszugänge
9. Technisches Fehlverhalten und höhere Gewalt
10. Soft- und Hardwareschwachstellen in der Lieferkette

Die genannten Bedrohungen hängen dabei u.a. mit den folgenden Defiziten zusammen:

- Vorhandene proprietäre Systeme mit veralteter und verwundbarer Software
- Keine Sicherheitsfunktionen in den Produktionsanlagen enthalten
- Nicht abgesicherte Zugänge (Beispiel: Wartungszugang) und fehlende Netzwerk-Segmentierung
- Integrität von übermittelten Daten ist nicht geschützt
- Überwachung und Alarmierung mit

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen und Geschäftsführer der DECOIT GmbH & Co. KG

Hilfe von Logs ist selten vorhanden
- Echtzeitanforderungen der Produktionsumgebung stehen teilweise in Konflikt mit Sicherheitsfunktionen wie Verschlüsselung, Intrusion Detection oder Antivirus-Scannern

Gegen einen Teil der Probleme gibt es inzwischen proprietäre Firewall- und VPN-Lösungen für Industrieanlagen einiger Hersteller. Als Beispiel können hier die Sicherheitsprodukte aus der SCALANCE-Reihe für Anlagen der Siemens AG angeführt werden. Diese Lösungen vernachlässigen jedoch die Überwachung der Integrität und Identität der beteiligten Systeme. Ohne die Berücksichtigung dieser zwei Faktoren ist es, besonders im Hinblick auf sogenannte Advanced Persistent Threats (APT), schwer sicherzustellen, ob ein System manipuliert wurde. Ein APT liegt dann vor, wenn ein Hacker zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreift, sich unter Umständen darin bewegt, gegebenenfalls ausbreitet und so Informationen sammelt oder Manipulationen vornimmt. Sobald ein Angreifer einmal im System ist, fällt es schwer, ihn überhaupt zu bemerken oder gar aufzuspüren.

Das Konzept des TCN

Die Architektur des Trusted Core Network (TCN) setzt auf etablierten Standards der Trusted Computing Group (TCG) auf und ist aktueller Gegenstand der Forschung. Dieser Ansatz wurde ursprünglich vom Fraunhofer SIT für die Absicherung von Produktionsanlagen entwickelt. Hierbei steht besonders die Hochverfügbarkeit im Vordergrund. Mit Hilfe des TCN (siehe Abbildung 1) kann die Identität von Netzknoten geprüft und ein gewünschter Zustand dieser Knoten gewährleistet werden. In einem Peer-to-Peer-Netz prüft dazu jeder Netzknoten die Identität und den Zustand der benachbarten Knoten. Innerhalb der TCN-Architektur wird hierzu das Protokoll Trusted Neighbourhood Discovery (TND) verwendet, mit dem alle aktiven Geräte in der direkten Umgebung gefunden werden können. Ausgelöst wird die Suche durch eine Trigger-Nachricht, die über ein Protokoll (zum Beispiel Link Layer Discovery Protocol, LLDP) an alle physischen Schnittstellen in periodischen Intervallen verschickt wird. Um durch diesen Mechanismus eine Denial-of-Service-Attacke (DoS) zu vermeiden, können nur Netzknoten diesen Trigger-Impuls auslösen, die einen gültigen Identitätsschlüssel und eine minimale Unterbrechung (Timeout) besitzen. Unter Einsatz eines unveränderlichen Vertrauensankers (Trusted Platform Module, TPM) kann ein System einen benachbarten Knoten identifizieren und danach den Ist-Zustand mit einem geforderten Soll-Zustand vergleichen. So werden Änderungen und Manipulationen erkennbar und entsprechende Warnungen (Reports) werden direkt an ein zentrales Monitoring weitergegeben. Die Ausbreitung von Angriffen oder das Infizieren mit Schadsoftware (Maleware) kann so effizient unterbunden werden.

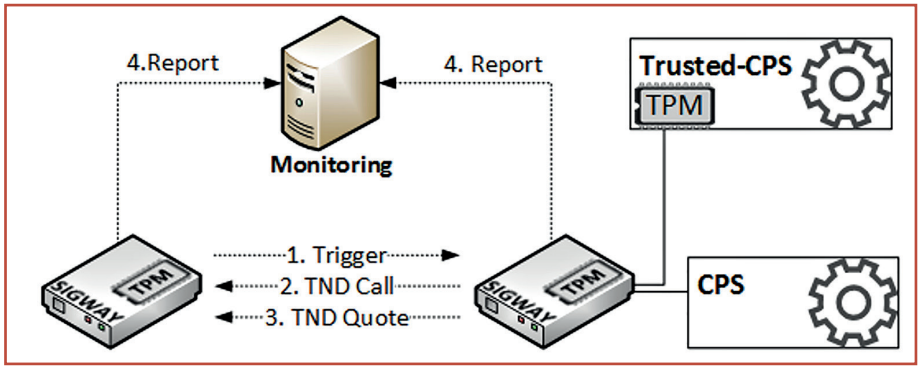

Abbildung 1: Mit Hilfe des TCN kann die Identität von Netzknoten ge-prüft und ein gewünschter Zustand dieser Knoten gewährleistet werden.

Durch die Überwachung der Geräte-Identität, installierten und ausgeführten Software sowie der Konfigurationsdaten, können Maßnahmen gegen erkannte Schwachstellen gezielt eingeleitet werden, so dass trotz des Fehlverhaltens einzelner Komponenten wichtige Funktionen aufrechterhalten werden (Resilienz). Wenn ein neues Gerät in ein TCN integriert wird, muss es entsprechend konfiguriert werden. Hierzu wird ein Protokoll zur Zero-Touch-Konfiguration verwendet, das auf den Sicherheitsfunktionen des TPM basiert, um ein effizientes Management zu ermöglichen. Für die Registrierung der Geräte wird daher lediglich eine eindeutige Gerätekennung benötigt. Nach der Integration des Gerätes durch einen Techniker in ein bestehendes TCN wird die Konfiguration, Registrierung usw. vollautomatisch durchgeführt. Eine Interaktion sollte nur im Fehlerfall notwendig sein.

Absicherung im TRUSTnet-Projekt

Die Basis einer sicheren Informations- und Kommunikationsinfrastruktur für Cyber-Physical Systems (CPS) ist die Sicherstellung der Identität und Integrität aller beteiligten, kritischen Systeme unter Nutzung eines Trusted Core Net-works (TCN) und der entsprechenden Absicherung aller Zugangskomponenten. Der in Abbildung 2 dargestellte Lösungsansatz des Projekts nutzt daher hardware-basierte Sicherheitstechnologien zur Identifikation und zum Schutz der Integrität von Industrieanlagen.

Um die IT-Sicherheit der TCN-Infrastruktur kontinuierlich zu überwachen, wird zusätzlich ein Security Information and Event Management (SIEM) Monitoring-System mit TCN-Interface entwickelt werden. SIEM-Lösungen können durch die Analyse von Loginformationen zusammenhängende Reports (Be-richte)

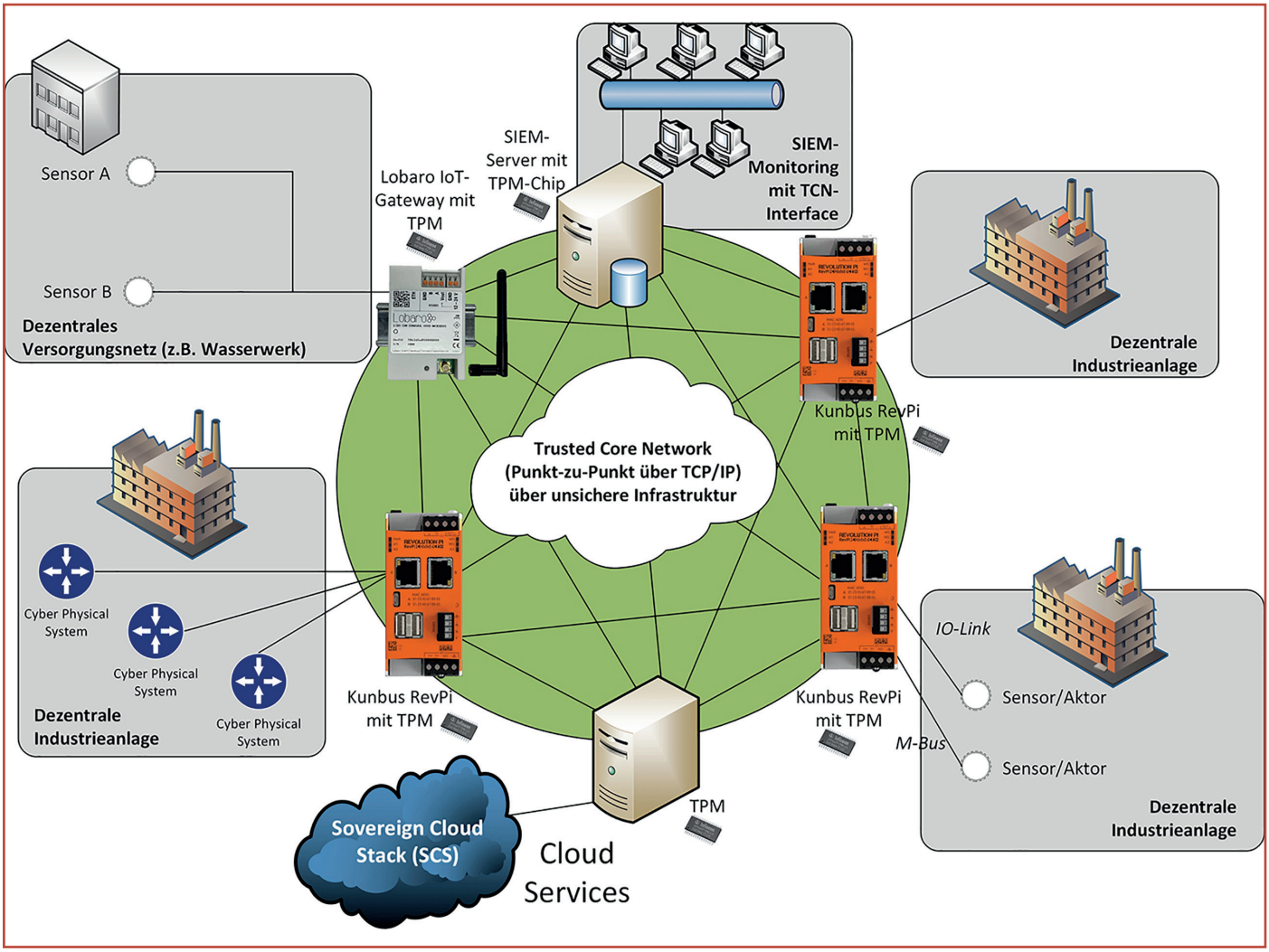

Abbildung 2: TRUSTnet-Szenario für die vertrauenswürdige Integration dezentraler kritischer Systeme. Um die IT-Sicherheit kontinuierlich zu überwachen, wird zusätzlich ein (SIEM) Monitoring-System mit TCN-Interface entwickelt

generieren. Diese Systeme kommen allerdings fast ausschließlich in großen Unternehmen zum Einsatz, da der Betrieb sehr komplex und kostenintensiv ist. Aktuelle SIEM-Systeme sind allerdings nur dann nützlich, wenn Experten in IT-Abteilungen die Sicherheitswarnungen und Ausgaben des SIEM-Systems richtig selektieren und interpretieren können, um dann geeignete Gegenmaßnahmen ergreifen zu können. Eine weitere Schwierigkeit liegt in proprietären Datenformaten für System-Ereignismeldungen (Events) und deren unterschiedlicher Aussagekraft. Durch den Einsatz von TPM-Chips kommen nun im Projekt neue Datenformate hinzu, die ausgelesen und mit anderen Events korreliert werden müssen.

Zur Vernetzung der Akteure werden im Rahmen des Forschungsprojekts dedizierte Systeme eingesetzt, die in der Lage sind, eine Grid-Infrastruktur nach dem Peer-to-Peer-Prinzip zwischen den Akteuren aufzubauen. Hierbei sind spezialisierte Kommunikationsgateways in der Lage, die einzelnen Verbindungen zu verwalten und ein Datenmanagement zu betreiben, um jedem Akteur nur die Daten zur Verfügung zu stellen, die er auch benötigt und zu denen er entsprechend berechtigt ist. In diesen Gateways ist ein TPM-Chip integriert, der als Vertrauensanker (Root-of-Trust) dient und Funktionen für das Identitätsmanagement und die Integritätskontrolle bereitstellt. Mit Hilfe des TPM sind die einzelnen Gateways in der Lage, vertrauenswürdige Verbindungen zwischen den Akteuren aufzubauen. Dabei ist es notwendig, jedem Akteur zu gewährleisten, dass die Komponenten, zu denen eine Verbindung aufgebaut wird, nicht manipuliert wurden und Schaden durch diese Komponenten ausgeschlossen ist. Die Gateways nutzen aus diesem Grund den TCN-Ansatz und können ihre Systemintegrität während des Verbindungsaufbaus und, wenn notwendig, in zeitlichen Abständen über eine bestehende Verbindung gegenseitig validieren. Hierdurch bilden diese ein vertrauenswürdiges Peer-to-Peer-Netz auf der Basis von TCP/IP zwischen den Akteuren. Bisher wurde das Konzept nur in idealen Umgebungen überprüft, was im Rahmen dieses Forschungsprojektes geändert werden soll. Ein Problem ist dabei die steigende Komplexität der in realen

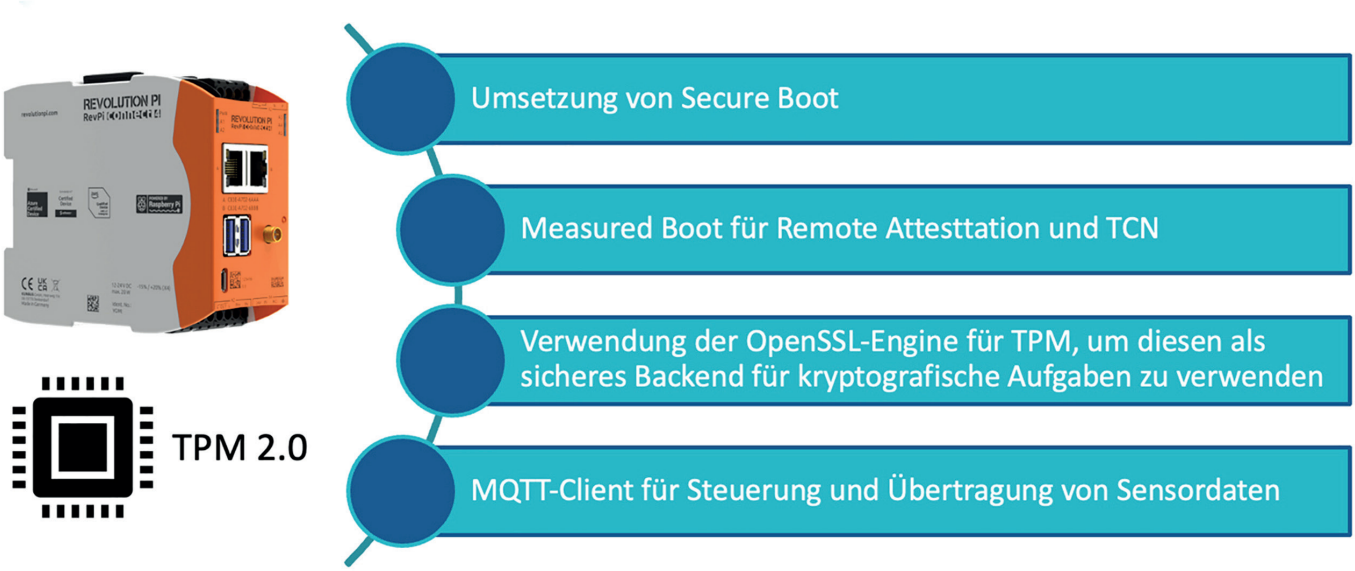

Abbildung 3: Die Absicherung eines einzelnen Gateways durch die Verwendung von Secure und Measured Boot mittels TPM-Nutzung. Als sicheres Backend wird die SSL-Verschlüsselung und MQTT-Verbindungen verwendet (Bilder: Detken)

Anlagen abzusichernden IKT-Strukturen, die eine realitätsnahe Umsetzung solcher Forschungsvorhaben immer schwieriger macht, zumal mögliche Sicherheits- und Stabilitätsprobleme bei dem Zusammenspiel verschiedener Komponenten oftmals nur bei der Betrachtung im Gesamtsystem auftreten.

Abbildung 3 zeigt die Absicherung eines einzelnen Gateways durch die Verwendung von Secure und Measured Boot mittels TPM-Nutzung. Als sicheres Backend wird die SSL-Verschlüsselung und MQTT-Verbindungen verwendet. Gegen Manipulationen an der Firmware durch direkten physischen Zugriff wird Secure Boot hier eingesetzt, während die Manipulationen von außerhalb durch Measured Boot verhindert werden kann. Das Protokoll Message Queuing Telemetry Transport (MQTT) ist ein Nachrichtenprotokoll für eingeschränkte Netzwerke mit geringer Bandbreite und IoT-Geräte mit extrem hoher Latenzzeit. Es ist daher auf Umgebungen mit niedriger Bandbreite und hoher Latenz spezialisiert. Aber auch bei Internet-of-Things(IoT)-Geräten, die keinen TPM-Chip enthalten, hat sich das Projekt etwas einfallen lassen. Als Alternative wird an der Umsetzung der Spezifikation Device Identifier Composition Engine (DICE) gearbeitet. DICE ist ein Hardware-Vertrauensanker (Root-of-Trust), der zum Schutz von Geräten und Komponenten eingesetzt wird, bei denen ein TPM-Chip unpraktisch oder nicht durchführbar ist. Wenn ein TPM vorhanden ist, kann DICE zusätzlich verwendet werden, um die Kommunikation mit dem TPM zu schützen und die Root-of-Trust-for-Measurement (RoTM) für die Plattform bereitzustellen. DICE wurde entwickelt, um kritische Lücken in der IT-Infrastruktur zu schließen und dabei zu helfen, Schutzmaßnahmen für Geräte zu etablieren. DICE-RoTM lässt sich zudem problemlos in bestehende IT-Infrastrukturen integrieren, da die Architektur flexibel und mit bestehenden Sicherheitsstandards kompatibel ist.

Um Remote-Attestation zu ermöglichen, wird im Projekt nicht mehr der Ansatz Trusted Network Communications (TNC) der TCG verwendet, weil TNC inzwischen zu viele Altlasten besitzt. Stattdessen wird auf das neu spezifizierte Informationsmodell des Trusted Attestation Protocol (TAP) gesetzt, welches protokollneutral ist. Es kann in Protokollen verwendet werden, die Zugang zu Netzwerken über VPN, SSH oder andere Protokolle ermöglichen. TAP liefert die grundlegenden Informationen, die für eine Beurteilung der Integrität eines Endpunkts auf der Grundlage von TPM-PCR-Werten oder mittels DICE-Signatur notwendig sind. Es kann mit den TPM-Chips der Versionen 1.2 oder der neueren Version 2.0 verwendet werden. Zwei-Wege- oder Ein-Wege-Protokolle lassen sich ebenfalls nutzen. Das TAP-Protokoll wird daher im TRUSTnet-Projekt genutzt, um Remote Attestation-Daten mit dem TPM und DICE zu übertragen.

Fazit

Zusammenfassend soll im TRUSTnet-Projekt ein TCN für den Einsatz in dezentralen Versorgungsnetzen konzipiert, implementiert und validiert werden, um die erhöhten Sicherheitsanforderungen zu erfüllen und als Vorlage (Blaupause) für andere, ähnlich strukturierte Anwendungen dienen kann. Damit würde man in Industrie4.0-Netzen den IT-Sicherheitsgrad signifikant erhöhen. Die Gateways, Protokolle und TPM-Chips sind auf jeden Fall dafür vorhanden. Jetzt muss nur noch die Bereitschaft für den Einsatz in der Industrie wachsen, denn durch TCN wird die Infrastruktur auf jeden Fall komplexer.