Trustpoint: Digitale Identitäten für eine sichere Industrie

Inhaltsverzeichnis

Kurzfassung

Das Projekt "Trustpoint" wurde im September 2023 vom Campus Schwarzwald, mittelständischen Unternehmen (PrimeKey Labs GmbH, asvin GmbH, achelos GmbH) und der Hochschule Hamm-Lippstadt gestartet. Das Projekt wird von ARBURG GmbH + Co KG, HOMAG GmbH, FANUC Deutschland GmbH, PHOENIX CONTACT GmbH & Co. KG und Siemens AG als assoziierte Partner unterstützt. Ziel des Projekts ist die Entwicklung einer Open-Source-Lösung zur sicheren Verwaltung digitaler Identitäten von Maschinen und Komponenten im industriellen Umfeld. Trustpoint wird vom Bundesministerium für Bildung und Forschung im Rahmen der Initiative KMU-innovativ mit 1,41 Mio. € gefördert.

Hintergrund und Motivation

Der Hintergrund und die Motivation für das Projekt Trustpoint liegen in der sich verändernden industriellen Landschaft und den damit verbundenen Anforderungen an die IT-Sicherheit. Die fortschreitende Digitalisierung von Maschinen und Anlagen hat zu erheblichen Veränderungen in der Operational Technology (OT) und den industriellen Prozessen geführt. Ausschlaggebend hierfür sind mehrere Mechanismen:

- **Veränderungen in der Industrie**: Die Digitalisierung hat die traditionelle Industrie in Richtung hochautomatisierter, vernetzter und intelligenter Betriebsumgebungen transformiert. Dies betrifft nicht nur die Produktion, sondern auch die gesamte Lieferkette.
- **IT-Sicherheit im Fokus**: Mit zunehmender Vernetzung und Automatisierung rückt die IT-Sicherheit in den Vordergrund. Industrielle Umgebungen sind zunehmend anfällig für Cyber-Bedrohungen, weshalb die Gewährleistung der Sicherheit zu einer Priorität geworden ist.
- **Maschinenidentitäten und Normen**: Die Verwendung von Maschinenidentitäten, wie sie in Standards wie OPC UA und IEC 62443 beschrieben sind, hat an Bedeutung

gewonnen. Diese Identitäten spielen eine entscheidende Rolle für die Sicherheit und Integrität von Kommunikation und Daten in industriellen Netzwerken.

- **Notwendigkeit von Authentifizierung und Rückverfolgbarkeit**: Maschinenidentitäten ermöglichen die Authentifizierung, die Validierung von Software, den Nachweis der Herkunft von Komponenten und die Schaffung einer sicheren Rückverfolgbarkeit. Diese Faktoren sind entscheidend für das Vertrauen zwischen Herstellern und Betreibern.
- **Herausforderungen im industriellen Umfeld**: Industrielle Umgebungen weisen spezifische Einschränkungen auf, die das Management von digitalen Zertifikaten und kryptographischen Schlüsseln erschweren. Dazu gehören Netzwerksegmentierung, eingeschränkte Konnektivität, begrenzte Hardware- und Software-Ressourcen, hohe Netzwerkdynamik und organisatorische Einschränkungen.

Herausforderungen

Diese Herausforderungen sind eng mit den spezifischen Anforderungen und Einschränkungen von Fabriken, Maschinen und industriellen Netzwerken verbunden. Im Folgenden werden einige der wichtigsten Herausforderungen im Einzelnen aufgeführt:

In industriellen Umgebungen sind Netzwerke oft stark segmentiert und weisen häufig eine eingeschränkte Konnektivität zu IT-Systemen auf. Diese Segmentierung und eingeschränkte Konnektivität erschweren die nahtlose Integration in erweiterte Wertschöpfungsnetzwerke. Mit der Ausweitung interner Netzwerke auf externe Partner, Kunden und Lieferanten wird es immer dringlicher, Vertrauen zu weiteren Einheiten über die Fabrikgrenzen hinaus aufzubauen.

Hard- und Software in industriellen Umgebungen unterliegen verschiedenen Einschränkungen. Die Aktualisierung von Software und Firmware erfolgt oft nur unregelmäßig und die Lebensdauer von Komponenten in Maschinen ist deutlich länger als die von herkömmlichen IT-Komponenten. Begrenzte Hardwareressourcen in diesen Umgebungen erschweren die Implementierung kryptographischer Funktionen, und oft fehlen sichere Speichermöglichkeiten für kryptographisches Material.

Industrielle Netzwerke sind von Natur aus dynamisch. Geräte treten häufig in das Maschinen- oder Fabriknetz ein oder aus ihm aus, was das Identitätsmanagement erschwert.

Organisatorisch verfügen viele Unternehmen, seien es Hersteller oder Betreiber von Maschinen und Komponenten, nicht über die notwendigen Kompetenzen und Ressourcen, um umfassende Sicherheits- oder Identitätskonzepte zu entwickeln und umzusetzen.

Der Nachweis von Ereignissen im Lebenszyklus einer Maschine erfolgt häufig manuell und ist lückenhaft. Fälschungssicherheit und eindeutige Rückverfolgbarkeit sind jedoch entscheidend für die Vertrauensbildung zwischen Herstellern und Betreibern.

Die Interoperabilität zwischen Herstellern und Betreibern sowie zwischen verschiedenen Herstellern ist häufig nicht gegeben. Die Betreiber haben Schwierigkeiten, die von den Herstellern eingebrachten Identitäten effektiv zu verwalten und zu überwachen, um den ordnungsgemäßen Betrieb der Maschinen zu gewährleisten.

Systeme mit langlebigen Komponenten erfordern kryptographische Mechanismen, die langzeitsicher oder zumindest austauschbar sind.

Lösungsansatz

Trustpoint verfolgt einen innovativen Ansatz, um die Herausforderungen bei der Verwaltung von Maschinenidentitäten in industriellen Umgebungen zu bewältigen. Im Mittelpunkt steht die Entwicklung eines Vertrauensankers, der es ermöglicht, digitale Identitäten von Maschinen über ihren gesamten Lebenszyklus hinweg sicher und effizient zu verwalten.

Die Lösung umfasst verschiedene Schlüsselfunktionen:

- **Signaturen und PKI-Dienste**: Trustpoint bietet die Möglichkeit, Signaturen zu prüfen und zu erstellen sowie PKI-Dienste (Public Key Infrastructure) bereitzustellen. Damit wird die Integrität und Authentizität von Kommunikation und Daten sichergestellt.
- **Onboarding und Bootstrapping Verfahren**: In Trustpoint werden Standards wie BRSKI (Bootstrapping Remote Secure Key Infrastructure), OPC UA Part 21 und FIDO FDO (Fast Identity Online Device Onboarding) betrachtet und bewertet. Die Integration der Mechanismen orientiert sich an den Bedürfnissen der Industrie.
- **Device Identification**: Die Lösung ermöglicht die eindeutige Identifizierung von Geräten und Komponenten, was für die Sicherheit und Rückverfolgbarkeit von entscheidender Bedeutung ist.
- **Risk Monitoring/Mitigation Tool**: Trustpoint bietet ein Tool zur Überwachung und Minimierung von Sicherheitsrisiken in industriellen Umgebungen. Damit können Unternehmen potenzielle Bedrohungen frühzeitig erkennen und bewältigen.

Der ganzheitliche Ansatz von Trustpoint zielt darauf ab, die Integration von Maschinen und Komponenten in industrielle Netzwerke sicherer und effizienter zu gestalten. Durch die Unterstützung von Authentifizierung, Verschlüsselung, Rückverfolgbarkeit und Risikomanagement leistet Trustpoint einen wesentlichen Beitrag zur Verbesserung der Sicherheit und Effizienz industrieller Prozesse.

Onboarding und Bootstrapping

Ein wesentlicher Aspekt des Trustpoint-Projekts ist die Integration von Onboarding- und Bootstrapping-Verfahren, die in Standards wie BRSKI (Bootstrapping Remote Secure Key Infrastructure), OPC UA Part 21 und FIDO FDO (Fast Identity Online Device Onboarding) beschrieben sind. Diese Verfahren spielen eine zentrale Rolle bei der sicheren Integration von Geräten in industrielle Netzwerke und bei der Bereitstellung digitaler Identitäten.

Trustpoint untersucht die Prinzipien von BRSKI (Bootstrapping Remote Secure Key Infrastructure), um ein sicheres Onboarding von Geräten in Netzwerke zu gewährleisten. Dieser Prozess ermöglicht es, Maschinen und Komponenten sicher und effizient in ein Netzwerk zu integrieren, indem sichergestellt wird, dass sie über die notwendigen Identitäten und Schlüssel verfügen, um sich zu authentifizieren und sicher zu kommunizieren. Diese Integration erleichtert

den Aufbau von Vertrauen zwischen den Geräten und dem Netzwerk.
Als weiteren Ansatz für ein sicheres Onboarding wird sich Trustpoint an den Methoden von OPC UA Part 21 orientieren, um eine sichere Integration von Geräten in OPC UA-basierte Netzwerke zu ermöglichen. Dieser Standard bietet Richtlinien und Empfehlungen für die sichere Konfiguration und Kommunikation von OPC UA Clients und Servern.
Das FIDO FDO (Fast Identity Online Device Onboarding) Verfahren wird ebenfalls in Trustpoint betrachtet. Es ermöglicht die sichere Registrierung und Aktivierung von Geräten, um deren Identität zu verifizieren und die Integration in Netzwerke zu vereinfachen. Dieser Prozess stellt sicher, dass nur vertrauenswürdige Geräte Zugang zum Netzwerk erhalten.

Innovation und Perspektiven

Eine der wichtigsten Innovationen ist die Verbesserung von Sicherheit und Effizienz. Trustpoint wird es Unternehmen ermöglichen, Maschinen und Geräte sicher in Netzwerke zu integrieren und zu betreiben. Dies wird zu einer erheblichen Verbesserung der Sicherheit führen, indem das Vertrauen zwischen Komponenten und Netzwerken gestärkt wird. Gleichzeitig wird die Effizienz und Flexibilität industrieller Prozesse erhöht, was wiederum die Wettbewerbsfähigkeit steigert.

Ein weiterer innovativer Aspekt von Trustpoint ist die Förderung nahtloser Kommunikation. Durch die Schaffung eines sicheren Vertrauensankers wird Trustpoint eine nahtlose und vertrauenswürdige Kommunikation zwischen verschiedenen Akteuren entlang von Wertschöpfungsketten ermöglichen. Dies wird die Interoperabilität verbessern und die Zusammenarbeit zwischen Herstellern, Betreibern und anderen Partnern in industriellen Umgebungen erleichtern.

Darüber hinaus leistet das Projekt einen wichtigen Beitrag zur sicheren Gestaltung des digitalen Wandels im industriellen Umfeld. Damit wird nicht nur die Zukunftsfähigkeit des Industriestandortes Deutschland gestärkt, sondern auch die digitale Souveränität der Unternehmen gewährleistet.