FABOS

Secure Update

Ausgangssituation

Gerätehersteller wollen Updates für Geräte, die beim Kunden im Einsatz sind, aus der Ferne installieren. Der Aktualisierungsprozess muss dabei gegen externe Einflüsse geschützt werden: Firmware-Images oder andere Daten müssen vor der Bereitstellung auf ihre Integrität hin überprüft werden. Die Verwendung von Public-Key-Verschlüsselung und sicheren Hardware-Elementen in einer separaten Secure-Update-Partition auf einem Echtzeit-Hypervisor wie PikeOS ermöglicht das Herunterladen und Installieren von Updates für die SPS, die auf demselben Gerät läuft.

Lösungsansatz

Ziel ist es, einen Aktualisierungsmechanismus wie in NE 177 beschrieben zu integrieren. Namur NE 177 definiert eine mehrstufige Architektur für speicherprogrammierbare Steuerungen (SPS) mit Bereichen mit unterschiedlichem Zugang in Sicherheitsstufen. Die Namur-Empfehlung (NE) 177 definiert die Sicherheitsanforderungen und die Architektur eines sicheren Gateways. Die Namur-Sicherheitsanforderungen basieren auf der IEC 62443-4-2, die funktionale Anforderungen beschreibt und die Verwendung von Zonen und Conduits als Lösung für die technische Sicherheit von IACS-Komponenten (Industrial Automation and Control System) vorschlägt. Der Zweck der Zonen ist es, die sicherheitskritische Komponente wie den Kernprozess von allen anderen Prozessdomänen zu trennen. Die offene Namur-Architektur beschreibt drei Zonen, nämlich Kernprozesssteuerung (CPC), Überwachung und Optimierung (M&O) intern und M&O extern mit unterschiedlichen Anforderungen an die Sicherheitsstufe (SL). Die sicherste Stufe namens „Core Process Control“ führt die SPS-Emulation selbst aus und veröffentlicht Daten in der Cloud und bietet keinen Zugriff mit einer Ausnahme, einer sicheren Aktualisierung des vom SPS-Emulator ausgeführten Steuerungsprogramms. Diese Sicherheitszonen ermöglichen die Integration von IT-Technologien und Betriebssystemen für die Prozessindustrie, die nicht den hohen Sicherheitsanforderungen der Automatisierungspyramide entsprechen, ohne dass die Prozesssicherheit beeinträchtigt wird.

Unser Leistungsangebot

Die sichere Update-Plattform nutzt eine MILS-Architektur (Multiple Independent Levels of Security) für sichere Software-Updates. Die Grundlage der Architektur ist die hardwarebasierte Root-of-Trust-Komponente mit dem entsprechenden Software-Stack. Die Sicherheitsplattform besteht aus drei Ebenen: Anwendung, Hypervisor (Isolierung auf Systemebene) und Hardware-Sicherheitselement. Auf der Anwendungsebene lädt der Update-Manager die Updates von einem entfernten Server über ein sicheres Update-Protokoll herunter. Der PikeOS-Hypervisor stellt die zentrale Schicht der Sicherheitsplattform dar und definiert Schnittstellen für die Integration von Secure Elements (SE). Der Demonstrator umfasst Folgendes:

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

DLR Projektträger

aufgrund eines Beschlusses des Deutschen Bundestages

- Abgesicherter Updateprozess der kritischen PLC-Komponenten über unsichere Netze
- Signierte und verschlüsselte Update-Pakete
- Data Diode zwischen I/O Teil des Updaters und dem Prüfen und Verteilen des Updates
- Data Diode zwischen Publisher und Netzwerk Komponente zur Kommunikation mit z. B. der Cloud

Einordnung ins Gesamtprojekt FabOS

Jeden Tag werden wir Zeugen neuer raffinierter Angriffe auf industrielle Systeme, Kraftfahrzeuge, medizinische Geräte usw., die den Bedarf an integrierter Sicherheit erhöhen. Die Gerätesicherheit wurde in Normen wie IEC 62443 und der Namur-Sicherheitsarchitektur behandelt, welche die funktionalen Sicherheitsanforderungen für industrielle Kontrollsysteme beschreiben. Daher ist die Sicherheit ein Bestandteil der FabOS-Referenzarchitektur. Die Identifizierung und Authentizität des Benutzers oder der Benutzerin und der Software wurden nachgewiesen.

Ihr Nutzen

Die verwendeten Komponenten geben die folgenden Vorteile

- Sicheres Design und Architektur auf der Grundlage von IEC 62443 und Namur-Sicherheitsarchitektur
- Sicherheit durch Design auf der Grundlage der MILS-Architektur
- Ein Hardware-Sicherheitsmodul wie ein secure element (SE) wird verwendet, um die für den Aktualisierungsprozess erforderlichen Sicherheitseigenschaften (Schlüsselspeicherung, Verschlüsselung und Authentifizierung) zu implementieren
- Sicheres Software-Update über das Internet
- Abgesicherter Updateprozess der kritischen PLC-Komponenten über unsichere Netze

Zielgruppe

Unternehmen, die Geräte herstellen.

Werden Sie Teil der FabOS-Community

Ein Betriebssystem für die Produktion klingt interessant für Sie? Entweder weil Sie es gerne bei sich einsetzen würden oder Sie gerne bei der Entwicklung mitwirken würden?

Dann melden Sie sich für die FabOS-Community an und begleiten Sie unser Projekt:

www.fab-os.org/werde-partner

- Regelmäßige Informationen zu Neuigkeiten aus dem Projekt
- Kostenlose und bevorzugte Teilnahme an unseren Workshops
- Direkte Möglichkeit, Anforderungen und Feedback einzubringen
- Zugang zu Datensätzen und Vorlagen für Verwaltungsschalen
- Frühzeitige Erprobung entwickelter Projektsoftware

Wir freuen uns auf den Austausch und hoffen, Sie bald als assoziierten Partner im Projekt willkommen heißen zu dürfen.

Folgende Projektpartner sind an dem Exponat beteiligt:

Ansprechpartner:

SYSGO GmbH
Am Pfaffenstein 8 | 55270 Klein-Winternheim
Deutschland

Dr. Ing. Zeeshan Ansar
Tel.: +49-6136-9948-932
zeeshan.ansar@sysgo.com

info@fab-os.org | www.fab-os.org

EMBEDDING INNOVATIONS