SEIZE

Secure Edge Devices For Industrial Zero-Trust Environments

Programm / Ausschreibung	Bridge, Bridge - ÖFonds, 33. Ausschreibung BRIDGE 1 (Ö-Fonds 2019)	**Status**	laufend
Projektstart	01.01.2022	**Projektende**	31.12.2024
Zeitraum	2022 - 2024	**Projektlaufzeit**	36 Monate
Keywords	Industrial Internet of Things, Cybersecurity, Security Architectures, Enclaves, Side Channels		

Projektbeschreibung

Das industrielle Internet der Dinge (IIoT) eröffnet enorme Möglichkeiten im Bereich der intelligenten Produktion, aber führt gleichzeitig auch zu fundamentalen Herausforderungen bezüglich Cybersicherheit. Im Kern stellt das IIoT eine äußerst heterogene Umgebung mit geteilten Netzwerken, geteilter Hardware und geteilter Software dar, welche durch die Konvergenz von IT Systemen mit industrieller Infrastruktur entsteht. Besonders relevant bezüglich Sicherheit sind industrielle Edge Devices, die dazu eingesetzt werden um industrielle Komponenten mit dem Internet zu verbinden. Hierdurch werden diese allen Arten von Cyberbedrohungen ausgesetzt. Die Absicherung des IIoT ist eine ungelöste und vielschichtige Herausforderung: Viele unterschiedliche Akteure wie Gerätehersteller, Anlagenbetreiber und Softwareanbieter wollen ihre Assets (z. B. Sensordaten, Steuerungssoftware, geistiges Eigentum) vor Cyberangriffen schützen - idealerweise ohne gegenseitige Abhängigkeiten bezüglich Sicherheit.

Das Ziel des SEIZE Projekts ist es die Grundlagen für die Absicherung des IIoT zu erforschen. Es geht darum neue Konzepte und Methoden zu finden um Kontrollsoftware authentisch ausführen zu können und Abhängigkeiten bezüglich Cybersicherheit zwischen den Akteuren zu minimieren. Das Projekt fokussiert auf zwei Hauptthemen.

Erstens werden starke Isolationstechniken erforscht, welche es erlauben, kritische (Steuerungs-)Software zu isolieren und dadurch nicht benötigte Vertrauensbeziehungen aufzulösen. Dazu werden zwei komplementäre Isolationstechniken betrachtet, nämlich Enklaven und Sandboxen, welche beide im IIoT Kontext benötigt werden. Enklaven helfen dabei, kritische (Steuerungs-)Software vom Rest des Systems abzuschirmen und erlauben z.B. den Schutz gegen ein kompromittierten Betriebssystem. SEIZE untersucht nicht nur die aktuellen Einschränkungen von Enklaven, sondern erforscht auch neue Erweiterungen und Generalisierungen. Sandboxen bieten das umgekehrte Schutzmodell und helfen dabei, gefährlichen Code (z. B. von Drittanbietern) einzusperren. Die meisten Sandboxing-Techniken wurden jedoch noch nicht in Verbindung mit Enklaven untersucht. In SEIZE geht es darum auch Einschränkungen von Sandboxing-Techniken auflösen und insbesondere auch Eklaven und Sandboxing-Techniken ineinander verschachteln.

Zweitens werden grundlegende Konzepte und Methoden erforscht, welche (Steuerungs-)Software gegen Laufzeitangriffe

unter Berücksichtigung der IIoT Rahmenbedingungen absichern können. Insbesondere geht es beispielsweise um die Verhinderung von Softwareschwachstellen durch Memory Safety und Kontrollflussintegrität. Im industriellen Umfeld gibt es andere Anforderungen und Einschränkungen als im Bereich der klassischen IT. Diese eröffnen auch das Potential für neue Sicherheitsmechanismen mit geringeren Overheads. Dies wird im Projekt exploriert. Darüberhinaus benötigt kritische Steuerungssoftware authentische Interaktionen, z. B. mit Sensoren und Aktoren, wofür auch Verfügbarkeitsgarantien notwendig sind, die aktuelle Enklaventechnologie nicht bieten. SEIZE untersucht neuartige Enklavendesigns, welche die notwendige Authentizität für Steuerungsinteraktionen bieten und auch Denial-of-Service Angriffen standhalten.

SEIZE zielt darauf ab die entwickelten Methoden und Konzepte prototypisch umzusetzen und unter Laborumgebungen zu analysieren. Um realistischen industriellen Einschränkungen Rechnung zu tragen, ist des das Ziel die Laufzeitkosten für die Sicherheitsmechanismen auf 10-20% zu begrenzen.

Abstract

The industrial Internet of Things (IIoT) opens up enormous opportunities in the area of smart production, but also leads to fundamental security challenges. At its core, the IIoT presents a highly heterogeneous compute environment with shared networks, shared hardware, and shared software that arises from a convergence of traditional IT infrastructure with the industrial domain. Industrial edge devices require particular attention, as they typically connect previously isolated industrial components with the internet, thus exposing the IIoT to all sorts of cyberthreats. Securing the IIoT is an unsolved and multifaceted challenge: Multiple different stakeholders such as industrial manufacturers, plant operators, and software vendors all want to protect their assets (e.g., sensor data, control software, intellectual property) from cyberattacks - ideally without the need to rely on each other with respect to security.

The goal of the SEIZE project is to research the foundations for securing the IIoT by finding novel technologies to ensure authentic control and execution as well as to minimize the trust relations between the stakeholders and components of the IIoT. The project focuses on two main topics.

First, we research strong isolation techniques that give stakeholders the means to isolate their critical (control) software and, thus, break all unintended trust relations. We research two complementary isolation techniques, namely enclaves and sandboxes, both of which are needed to account for modern industrial use cases. Enclaves shield critical (control) software from the rest of the system and allow, e.g., to protect against a compromised operating system. We investigate not only their current limitations but also explore novel designs and generalizations to increases their flexibility and applicability to industrial settings. Sandboxes provide the inverse protection model and help stakeholders confine dangerous code (e.g., third-party libraries). However, most sandboxing techniques have not been studied in conjunction with enclaves. We aim at overcoming the current limitations of sandboxing techniques and to in particular also nest them with enclaves.

Second, we research foundational concepts and methods to allow stakeholders to secure their (control) software against runtime attacks while taking into account the complex requirements of the IIoT. In particular, vulnerabilities in the software need to be addressed via memory safety or control-flow integrity, for example. Compared to classical IT settings, further constraints apply to industrial compute environments. These constraints also offer the potential for dedicated countermeasures with reduced overheads that we intend to explore. Moreover, critical control software relies on the authenticity of its interactions, e.g., with sensors and actuators, for which it also requires availability guarantees, which

current enclave technologies fail to provide. We investigate novel enclave designs that provide the necessary authenticity for control interactions and that withstand denial-of-service attacks.

We aim for proof-of-concept prototypes of our methods and concepts that we analyze in lab settings. To account for realistic industrial constraints, we aim for an overall performance overhead for security mechanisms of no more than 10-20%.

Projektkoordinator

- Technische Universität Graz

Projektpartner

- Siemens Aktiengesellschaft Österreich