RAPID

Runtime Attestation for Protecting Industrial Devices (RAPID)

Programm / Ausschreibung	Bundesländerkooperationen TP, Oberösterreich, Security Technologies & Solutions	**Status**	laufend
Projektstart	01.01.2027	**Projektende**	31.12.2029
Zeitraum	2027 - 2029	**Projektlaufzeit**	36 Monate
Barwert der Projektförderung	€ 596.827		
Keywords	software attestation, industrial control systems, cybersecurity		

Projektbeschreibung

Angesichts immer ausgereifterer statischer Sicherheitsmechanismen für Server sowie eingebettete Industriesysteme, wie z. B. dem sogenannten „Secure Boot“ und damit verbundenen Integritätsprüfungen, verlagern Angreifer ihren Fokus zunehmend auf die dynamische Systemmanipulation zur Laufzeit. Diese Form der Kompromittierung ist besonders kritisch, da sie das tatsächliche Ausführungsverhalten betrifft und Beweise für den Angriff beim Ausschalten bzw. Neustart des Geräts oft rückstandslos verschwinden. Es ist daher unzureichend, lediglich einen unveränderten Offline-Zustand eines Systems zu garantieren; vielmehr muss die Konformität mit einem definierten Soll-Verhalten kontinuierlich im laufenden Betrieb sichergestellt werden.
Das vorliegende Projekt erforscht Methoden, um dieses Soll-Verhalten durch Laufzeit-Integritätsprüfung (Runtime Attestation) kryptografisch nachweisbar zu verifizieren. Dieser Ansatz schafft die notwendige Vertrauensbasis für eine sichere Vernetzung, indem beispielsweise die Integrität des beabsichtigten Empfängersystems sensibler Daten – etwa bei der Übertragung von Betriebsgeheimnissen oder personenbezogener Daten – in Echtzeit verifiziert wird. Gleichzeitig dient die Attestierung als technischer Nachweis angemessener Vorsichtsmaßnahmen des Senders im Sinne der IT-Sicherheit.
Die Umsetzung dieser Methoden soll in diesem Projekt gezielt im Bereich industrieller Steuerungssysteme erprobt werden, wobei das Anwendungsspektrum von integrierten Maschinensteuerungen bis hin zu komplexen Leitständen mit dedizierten Security-Agents reicht. Traditionell basiert die Sicherheit industrieller Anlagen oft auf physischer Abschirmung. Diese ist jedoch durch die zunehmende Vernetzung und Internetanbindung moderner Anlagen unzureichend, weshalb dringender Handlungsbedarf besteht. Eine zentrale Herausforderung bildet dabei die Ressourceneffizienz: Während Neusysteme typischerweise über Leistungsreserven verfügen, müssen Sicherheitslösungen auch auf Bestandssystemen sowie eingebetteten Systemen mit minimalen Ressourcen funktionieren, um flächendeckende Modernisierung ohne kompletten Hardwareaustausch und damit einhergehende signifikante Kosten zu ermöglichen.
Diese Entwicklungen gewinnen durch die gestiegenen Anforderungen regulatorischer Rahmenbedingungen wie NIS2 und den Cyber Resilience Act massiv an Bedeutung. Unternehmen müssen künftig nicht nur Sicherheitvorkehrungen erhöhen, sondern Angriffe aktiv erkennen und die Einhaltung von Sicherheitsstandards lückenlos nachweisen können. Die Beteiligung an diesem Projekt sichert den Zugang zu weltweit führender Spitzenforschung und verschafft den beteiligten Unternehmen

durch die frühzeitige Implementierung zukunftsweisender Sicherheitsstandards einen signifikanten Wettbewerbsvorteil.

Abstract

Given the increasingly sophisticated static security mechanisms for servers and embedded industrial systems such as Secure Boot and its associated integrity checks, attackers are shifting their focus to dynamic system manipulation at runtime. This form of compromise is particularly dangerous because it affects the actual execution behavior, and evidence of the attack often disappears completely when the device is powered off or restarted. Therefore, simply guaranteeing an unaltered offline state of a system is no longer sufficient. Rather, compliance with a defined expected behavior must be continuously ensured during operation.
This project explores methods to cryptographically verify this expected behavior through integrity checks at runtime (runtime attestation). This approach establishes the necessary foundation of trust for secure networking by verifying, for example, the integrity of the intended recipient system of sensitive data—such as when transmitting trade secrets or personal data—in real time. Simultaneously, the attestation serves as technical proof that the sender has taken appropriate cybersecurity precautions.
The implementations of these methods will be tested in this project specifically in the domain of industrial control systems, with the application spectrum ranging from integrated machine controls to large control stations, where dedicated security agents may be executed. Traditionally, the security of industrial plants is often based on physical separation. However, this is insufficient due to the increasing networking and internet connectivity of modern plants, which is why there is an urgent need for action. A key challenge here is resource efficiency: While new systems typically have performance reserves, security solutions must also work on legacy and embedded systems with minimal resources in order to enable comprehensive modernization without complete hardware replacement and the associated significant costs.
These developments are gaining massive importance due to the increased requirements of regulatory frameworks such as NIS2 and the Cyber Resilience Act. In the future, companies will not only have to increase cybersecurity precautions but also actively detect attacks and be able to provide complete proof of compliance with security standards. Participation in this project secures access to world-leading cutting-edge research and provides the participating companies with a significant competitive advantage through the early implementation of future-oriented security standards.

Projektkoordinator

- Universität Linz

Projektpartner

- Dynatrace Austria GmbH
- Software Competence Center Hagenberg GmbH
- Sprecher Automation GmbH
- System 7 Railtechnology GmbH