synERGY

security for cyber-physical value networks exploiting smart grid systems

Programm / Ausschreibung	IKT der Zukunft, IKT der Zukunft, IKT der Zukunft - 4. Ausschreibung (2015)	**Status**	laufend
Projektstart	01.01.2017	**Projektende**	31.12.2019
Zeitraum	2017 - 2019	**Projektlaufzeit**	36 Monate
Keywords	2_Cyber-Physische_Produktionssysteme		

Projektbeschreibung

Cyber Physical Systems (CPS), wie jene, die in Wertschöpfungsnetzwerken zur Realisierung einer verteilten Fertigung von Gütern Verwendung finden, sind anfällig für verschiedene Arten von Cyber-Attacken. Dies liegt unter anderem daran, dass zunehmend weit verbreitete commercial-off-the-shelf-Produkte (COTS) eingesetzt werden und CPS zunehmend auch über physische Organisationsgrenzen hinweg interagieren müssen. Der Grad der Komplexität moderner Cyber-Angriffen hat sich in den letzten Jahren stark zugenommen – in Zukunft werden Angreifer auch zunehmend CPS ins Visier nehmen. Bedauerlicherweise sind heutige Sicherheitslösungen, die für Enterprise-IT-Infrastrukturen verwendet werden, nicht ausreichend um CPS zu schützen, da CPS weitgehend unterschiedliche Eigenschaften aufweisen. Beispielsweise umfassen CPS stark heterogene Technologien und haben eine Architektur, die sehr spezifisch von den zu kontrollierenden physischen Prozesse geprägt ist. Außerdem kollidiert das Paradigma präventiver Security Technologien mit den hohen Safety-Anforderungen in CPS; zum Beispiel könnte das Blockieren verdächtigen Verhaltens in einer reinen Enterprise IT-Umgebung akzeptabel sein, aber mit Sicherheit nicht in zeit- und sicher-heitskritischen Umgebungen, die mit CPS synonym sind. Die Chancen von unerwünschten Nebenwirkungen sind enorm. Als Konsequenz müssen reaktive Sicherheitstechniken in CPS angewandt werden, die darauf beruhen Angriffe rechtzeitig und auf genaue Art und Weise zu erfassen. Um dies zu erreichen, insbesondere bei komplexen und verdeckten mehrstufige Angriffe wird ein Ansatz benötigt, der Informationen aus allen CPS Schichten korreliert, ein-schließlich des Feldbereichs, des SCADA-Backends, der Unternehmens-IT und des WANs (im Falle von ausgedehnten CPS). Allerdings arbeiten heutige Sicherheitslösungen in der Regel nur auf einzelnen Schichten und sind deshalb nicht in der Lage ein vollständiges Bild aufzunehmen. Dies führt zu einer eingeschränkten Sicht des Bedienpersonals in Bezug auf die Grundursache eines Angriffs, und daher ggf. zu einer Reduktion der Gesamtverfügbarkeit eines CPS.
Daher ist es das Ziel von synERGY neuen Methoden, Werkzeuge und Prozesse für Cross-Layer-Anomalieerkennung (AD) zu entwickeln, die die frühe Entdeckung von sowohl cyber- als auch physischen-Angriffe ermöglichen, die Auswirkungen auf die Sicherheit von CPS haben. Um dies zu erreichen, wird synERGY neuartige Machine Learning Ansätze erarbeiten, die das normale Verhalten eines Systems erfassen und Folgen von Sicherheitsverletzungen als Abweichungen vom Normverhalten erkennen können. Während dieses Konzept in der Regel für Enterprise-IT-Umgebungen aufgrund ihrer komplexen Verhaltensmuster ungeeignet ist, ist der Ansatz insbesondere für CPS in Wertschöpfungsnetzwerken sehr vielversprechend,

da diese ein eher deterministisches Verhalten haben. Die Lösung von synERGY passt sich flexibel an spezifische CPS Schichten an (z.B. durch dynamisches Hochsetzen von Schwellwerten zum Erkennen von Verhaltensabweichungen in Systemteilen mit sehr deterministischen Verhalten, aber Anwendung weniger strenger Regeln für andere Teile der zu schützenden Infrastruktur), um damit seine Erkennungsfähigkeiten zu verbessern. Darüber hinaus wird synERGY Schnittstellen zu verschiedenen Organisationsdatenquellen ausweisen, wie Asset-Datenbanken, Konfigurationsmanagement und Risikodaten (letzteres ist besonders für die flexible Überwachung der am stärksten gefährdeten Komponenten von Interesse). Das Ziel ist es, die halbautomatische Interpretation der detektierten Anomalien zu erleichtern, was insbesondere hilft die Anzahl von Fehlalarmen zu reduzieren und die Nütz-lichkeit von synERGY für den Betreiber zu erhöhen. Der synERGY-Ansatz wird in realen Smart-Grid-Umgebungen validiert werden – ein gesellschaftlich wichtiges CPS. Als "Nebenprodukt" dieser Bewertung planen wir Roh-Datensätze anderen Forschungsgruppen verfüg-bar zu machen (in Übereinstimmung mit synERGYs Daten-Management-Plan) um parallele Arbeiten zum Thema Anomalie-Erkennungssysteme zu unterstützen. Aufgrund des im Projekt gewählten modularen Ansatzes ist zu erwarten, dass die synERGY-Ergebnisse in einer breiten Palette von CPS in Wertschöpfungsnetzwerken anwendbar sein werden, und somit einen größeren Impact auf künftige CPS-Security-Lösungen haben werden.

Abstract

Cyber Physical Systems (CPS), e.g., those used in value-added networks to realize distributed manufacturing, are vulnerable to various kinds of cyber-attacks. This is because, amongst other reasons, they make use of commercial-off-the-shelf products to implement industrial control systems, and interact across organizational boundaries and physical borders. The degree of sophistication of modern cyber-attacks has increased in recent years – in the future, these attacks will increasingly target CPS. Unfortunately, today’s security solutions that are used for enterprise IT infrastructures are not sufficient to protect CPS, which have largely different properties, involve heterogeneous technologies, and have an architecture that is very much shaped to specific physical processes. Furthermore, preventive security techniques clash with the stringent safety requirements in CPS, e.g., blocking suspicious behaviour might be acceptable in an enterprise IT environment, but certainly not in time- and safety-critical environments that are synonymous with CPS. The chances of unwanted side-effects are enormous. As a consequence, reactive security techniques must be applied to CPS, which rely upon the ability to detect attacks in a timely and accurate manner. In order to achieve this, especially for complex and stealthy multi-stage attacks, an approach is required that correlates information from all CPS layers, including the field area, the SCADA backend, the enterprise IT and the WAN (in case of large-scale CPS). However, today’s security solutions usually address only single layers, and are not able to take account of the full picture. This leads to an operator having a limited view regarding the root cause of an attack, which can reduce the overall availability of a CPS.
Therefore, the objective of synERGY is to develop new methods, tools and processes for crosslayer Anomaly Detection (AD) to enable the early discovery of both cyber- and physical-attacks, which will have an impact on the security of CPS. To achieve this, synERGY will develop novel machine learning approaches to understand a system’s normal behaviour and detect consequences of security issues as deviations from the norm. While this concept usually fails for enterprise environments, because of their complex behavioural patterns, the approach is very promising for CPS in value networks that have a rather deterministic behavior. The solution proposed by synERGY will flexibly adapt itself to specific CPS layers (e.g., automatically applying more sensitive behaviour deviation thresholds to more deterministic system areas, and be less strict for other parts), thus improving its detection capabilities. Moreover, synERGY will interface with various organizational data sources, such as asset databases, configuration management, and risk data (the latter is especially of interest for flexible

monitoring of the most threatened components). The aim is to facilitate the semi-automatic interpretation of detected anomalies, which can help to reduce false positives and increase the utility of the system to an operator. The synERGY approach will be evaluated in real smart grid vendor environments – a societally important CPS. As a “byproduct” of this evaluation, we plan to make raw CPS data sets available (in compliance with synERGY’s data management plan) to other research groups working on new anomaly detection methods. We propose, because of the approach taken in the project, the synERGY results will be readily applicable to a wide range of CPS in value networks, and will thus result in broader impact on future CPS security solutions.

Projektkoordinator

AIT Austrian Institute of Technology GmbH

Projektpartner

Huemer iT-Solution Ges.m.b.H.

MOOSMOAR Energies OG

Energie AG Oberösterreich Telekom GmbH

Universität Klagenfurt

LINZ STROM GAS WÄRME GmbH für Energiedienstleistungen und Telekommunikation

Bundesministerium für Landesverteidigung

Technische Universität Wien