Ontology-Based Security Tool for Critical Cyber-Physical Systems

Abdelkader Magdy Shaaban
Austrian Institute of Technology
Center for Digital Safety & Security
Vienna, Austria
Abdelkader.Shaaban@ait.ac.at

Thomas Gruber
Austrian Institute of Technology
Center for Digital Safety & Security
Vienna, Austria
Thomas.Gruber@ait.ac.at

Christoph Schmittner
Austrian Institute of Technology
Center for Digital Safety & Security
Vienna, Austria
Christoph.Schmittner@ait.ac.at

ABSTRACT

Industry 4.0 considers as a new advancement concept of the industrial revolution, which introduces a full utilization of Internet technologies. This concept aims to combine diverse technological resources into the industry field, which enables the communication between two worlds: the physical and the cyber one. Cyber-physical Systems are one of the special forces that integrate and build a variety of existing technologies and components. The diversity of components and technologies creates new security threats that can exploit vulnerabilities to attack a critical system. This work introduces an ontology-based security tool-chain able to be integrated with the initial stages of the development process of critical systems. The tool detects the potential threats, and apply the suitable security requirements which can address these threats. Eventually, it uses the ontology approach to ensure that the security requirements are fulfilled.

KEYWORDS

Cyber-physical System, Security, Threats, Ontology

ACM Reference format:
Abdelkader Magdy Shaaban, Thomas Gruber, and Christoph Schmittner. 2019. Ontology-Based Security Tool for Critical Cyber-Physical Systems. In *Proceedings of 23rd International Systems and Software Product Line Conference - Volume B, Paris, France, September 9–13, 2019 (SPLC '19),* 3 pages.
https://doi.org/10.1145/3307630.3342397

1 INTRODUCTION

In recent years, industrial production has changed towards a smart manufacturing form based on the integration of both the Internet of Things (IoT) and the Cyber-Physical Systems (CPS). That introduces a new industrial revolution is called Industry 4.0. CPS integrates and builds on a variety of existing technologies and components such as robotics, industrial automation, big data, and cloud computing [1] [2].

The insecure communication protocols and outdated components generate new security issues which can jeopardize the data by different types of attacks. The security aims to protect computer systems and information from various illegal acts [2]. Furthermore, to build a secure system is important to:

- define the exact potential threats that threaten the system,
- identify the most suitable security requirements able to address the identified threats s and reduce the overall risk,
- verify and validate that the security requirements meet the actual security need,

This work introduces a security tool-chain based on the ontology approach to define the security weaknesses in critical CPS applications. It uses a systematic and standard approach, such as an information security management system ISMS [3] and IEC 62443 series [4], which provide a standardized methodology for building a secure infrastructure.

2 THE STRUCTURE OF THE ONTOLOGY-BASED SECURITY TOOL

The security issues in CPS can be generated from the diversity of interconnected components or the existence of legacy units in system architecture. To address the security weaknesses in a system is needed to manage a massive quantity of security requirements to build a secure infrastructure according to a systematic and standard approach. Figure 1 shows a simple Smart Factory application as a good example of CPS application. This example is defined in separate layers; each layer contains different components as follows:

Field Devices: this layer contains sensors for collecting data and actuators as robotic arms for welding, handling, painting, drilling, or other specific function.

Processing Units: this consists of smart devices to process the sensors data and send the suitable action to actuators.

Communication Units: this layer consists of communication devices such as gateways to transfer data over the network of the Smart Factory.

Cloud Storage: this consists of physical cloud storage to store data over the cloud.

Observation: this layer monitors products over long-run to compare production and conditions across the years.

The example contains one legacy gateway (Gateway2) and some insecure communication protocols. The security tool-chain is applied to this example to find potential threats, define the proper security requirements, and ensure that these requirements are fulfilled.

SPLC '19, September 9–13, 2019, Paris, France
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6668-7/19/09…$15.00
https://doi.org/10.1145/3307630.3342397

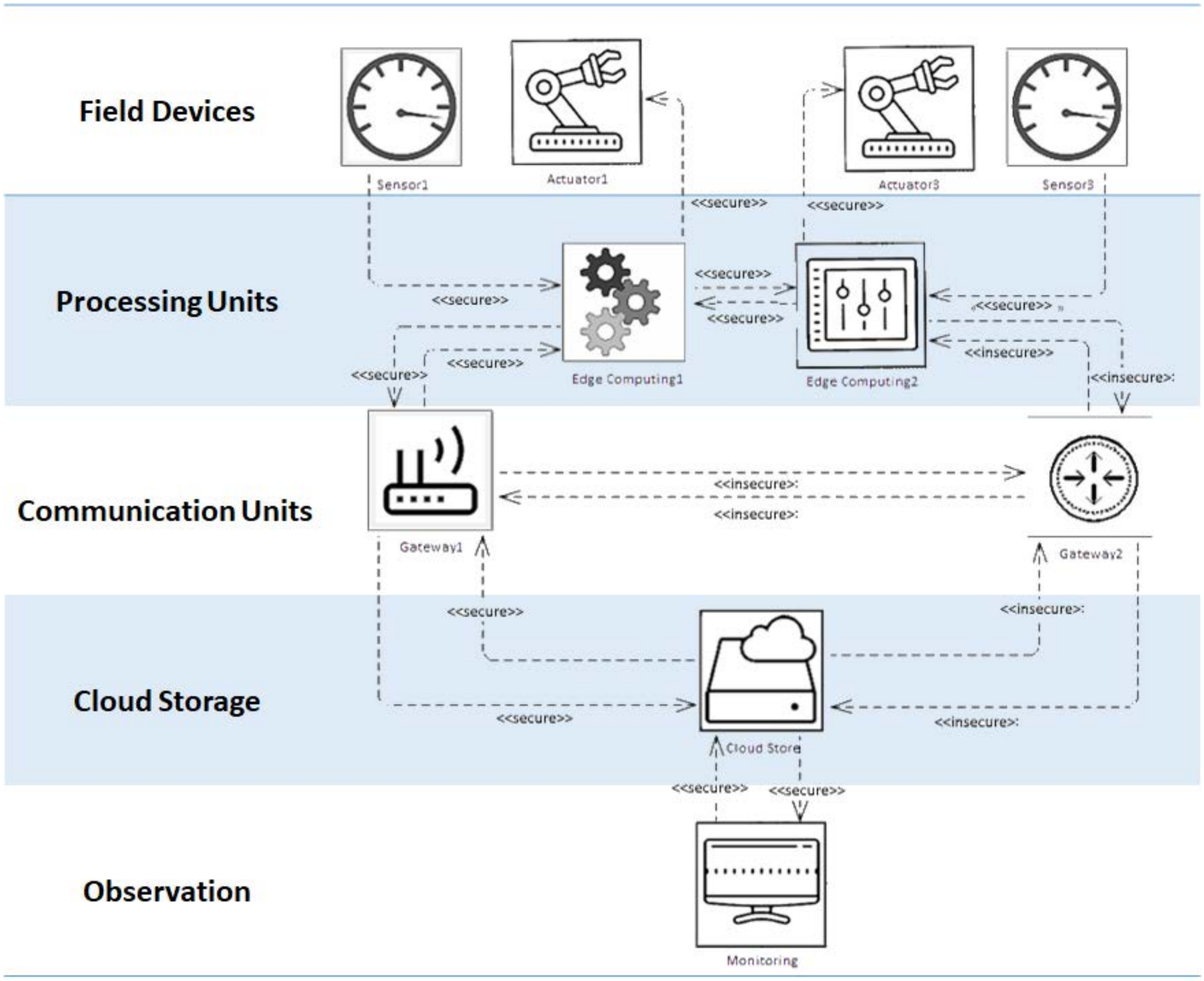

Figure 1: Smart factory example as a cyber-physical application

Figure 2 defines the main building blocks of the ontology-based security tool-chain (i.e., Threat Analysis, Security Requirements, Ontology Generator, and Security Testing).

2.1 Threat Analysis

Threat analysis is a method for analyzing and defining the potential threats which exploit the existing vulnerabilities in a system. The AIT Threat Management Tool (ThreatGet) is used in this phase to identify, describe, and understand several threats [5]. ThreatGet can be applied to a wide range of CPS applications such as smart factory, automotive, railways, networks, and others. The tool helps the system architect to:

- Build a secure CPS application,
- Identify security vulnerabilities,
- Identify threats and evaluate their risks.

In the analysis process, the tool uses the security configuration parameters of each unit in a system model. ThreatGet has a built-in threats catalog which contains a wide range of potential threats. The ThreatGet tool classifies the detected threats into six main groups according to the STRIDE model (i.e., Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege) [6].

ThreatGet is applied to the "Smart Factory" example to define and detect potential threats. The tool identifies 71 potential threats by scanning all elements and connectors in the model. The existence of a legacy Gateway (Gateway2) and insecure communication protocols lead to generating 26 potential threats out of the total detected threats.

The Ontology Generator collects the threats data (i.e., category, severity, and source and target units) and converts these data into ontology entities such as classes, subclasses, individuals, and properties. That will be used in the security testing process.

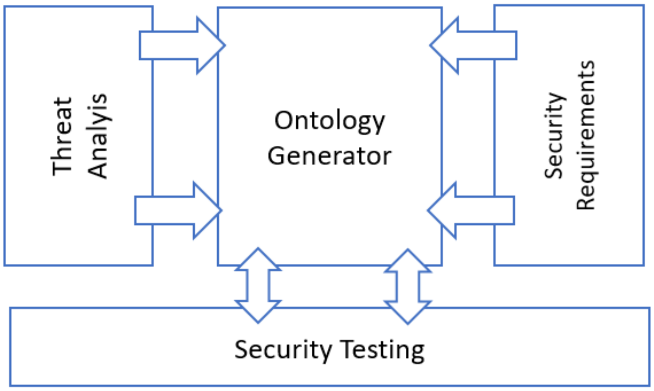

Figure 2: The building blocks of the ontology-based security tool-chain

2.2 Security Requirements

The security requirements play an essential role in any security engineering process. That aims to cover and handle the security weaknesses in a system to build a secure system according to a standardized model. The authors developed the Model-based Security Requirement Management Tool (MORETO) as a tool for security requirements analysis, allocation, and management using modeling languages such as SysML/UML. MORETO is an Enterprise Architect (EA) plugin for managing the IEC 62443 security standard [7] and IEEE 1686 security stand [8]. The primary purpose of the IEC 62443 series is to present a framework that addresses current and future security weaknesses in industrial systems and enables security risk management to the complete life cycle [4] [7]. IEEE 1686 describes the functions and characteristics to be implemented in Intelligent Electronic Devices (IEDs) to support Critical Infrastructure Protection (CIP) applications. The standard concerns the security issues according to the access, operation, configuration, firmware revision, and data retrieval from an IED [7]. The vulnerable element in this example is the Gateway2. MORETO selects 11 security requirements that must be applied to that example (Smart Factory) to handle the security weaknesses of the Gateway2.

The selected security requirements are presented in the ontological description to be used in the next phase to ensure that these requirements are fulfilled.

Security Testing

This phase uses the previously generated ontological representations of the identified potential threats and the selected security requirements to validate and verify the operational and the performance of the security requirements against the system security flaws. This phase creates an ontology linking between the hierarchical of threats and the security requirements nodes. This mapping process defines links between these two hierarchical ontologies, which represent that the selected security requirement can handle one or more of the detected threats.

Figure 3 shows the ontology representation of the detected threats on the "left-hand side," the selected security requirements on the "right-hand side," and the connections between these two hierarchies represent the security requirements are handled the security weaknesses (threats). That is considered as a comprehensive overview of all details of assets, detected threats, and related security requirements in the Smart Factory example. This comprehensive overview is called the Ontology Outlook. The security verification and validation process is achieved by using Ontology Security Testing Algorithm (OnSecta). The authors developed OnSecta as a rule engine performs logical rules from a set of asserted facts or axioms of threats and security requirements.

The algorithm performs security verification and validation in this example according to the current security status, and the actual security goal needs to be achieved. The Security Target (ST) is set during the concept phase to define a specific security goal. Therefore, the security requirements are used to mitigate the risk to an acceptable level. The resulting state is defined as Security Achieved (SA). The testing process completes if SA = ST; otherwise, OnSecta applies inference rules to the Ontology Outlook based on the value of SA and ST to finds additional security requirements that address threats. The security requirements are described in the ontology structure and stored in an Ontology Knowledge Base (KB).

First of all, the values of SA and ST have to be determined to define the current security state of the system (after applying the security requirements which are selected by MORETO) and to define the actual security target needs to be achieved. The value of ST can be determined by defining the maximum number of unacceptable risk severities in this example. We consider the threats with extreme severity are unacceptable, that means the ST = "the number of extreme threats." According to the identified potential threats, ThreatGet classifies 11 threads as extreme severity. Furthermore, the value of ST in this example equals 11.

OnSecta performs a series of queries to the Ontology Outlook to check which of the applied security requirements are fulfilled. According to the IEC 62443 security standard, the algorithm finds that the selected security requirements are addressed eight out of eleven extreme threats. The value of SA = 8 (SA <ST), and OnSecta should select additional security requirements until SA = ST.

2.3 Model Evaluation

The ontologies are considered the core of this work. That are used to represent data which are generated by ThreatGet and MORETO (threats and security requirements) to be used in the security testing process. OnSecta algorithm is applied to the Ontology Outlook to confirm that security requirements are meet the actual security target.

The following chart in Figure 4 describes the number of the selected security requirements of the Gateway2 (legacy device). MORETO and OnSects select the security requirements according to the IEC 62443-4-2, the technical security requirements for Industrial Automation and Control Systems Components (IACS) [4].

The IEC 62443 series provides detailed technical control system component requirements (CRs) associated with seven foundational requirements (FRs), there are a total of seven FRs [4] [9]:

- Identification and authentication control (IAC),
- Use control (UC),
- System integrity (SI),

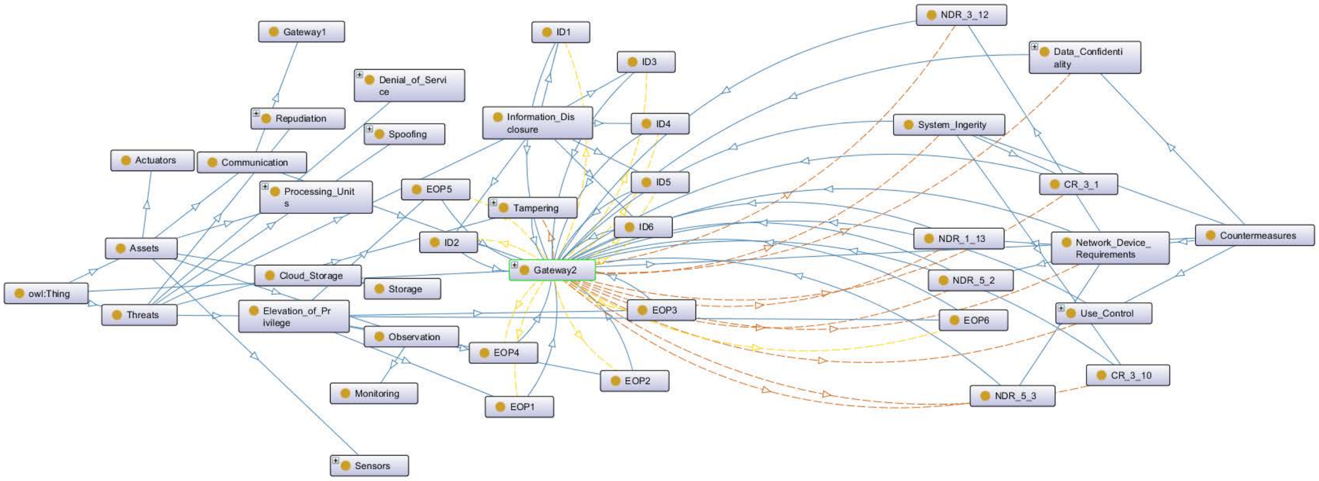

Figure 3: Ontology linking between threats (left) and security requirements (right)

- Data confidentiality (DC),
- Restricted data flow (RDF),
- Timely response to events (TRE),
- Resource availability (RA).

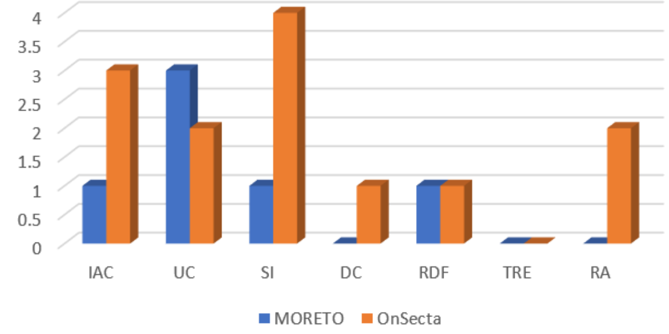

Figure 4: The number of the selected security requirements for the legacy Gateway2

The chart displays the number of security requirements according to the seven FRs which are selected to address the security weaknesses in the legacy device (Gateway2).

3 CONCLUSIONS

To conclude this contribution, the paper introduced a modern security tool-chain for critical CPS applications based on the ontology approach. The first phase in this chain is the ThreatGet. ThreatGet detects and identifies potential threats in critical systems. The second phase is MORETO tool as a security requirement management methodology to select security requirements to address the identified potential. The tool translates the data of threats and security requirements into ontological entities to be used in the security testing process. A smart factory example is used in this work to define the potential threats that can be generated from legacy components. The paper ends by identifying the number of the selected security requirements of legacy components (Gateway2) before and after applying the OnSecta.

OnSecta is still in the developing stage; the authors work on developing the different building blocks of OnSecta. Then, define a complete set of rules to perform security testing process.

ACKNOWLEDGMENT

This work has received funding from the AQUAS project, under grant agreement No. 737475. The project is co-funded by grants from Austria, Germany, Italy, France, Portugal and ECSEL JU.

REFERENCES

[1] Zhendong Ma, Aleksandar Hudic, Abdelkader Shaaban, and Sandor Plosz. Security viewpoint in a reference architecture model for cyber-physical production systems. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 153–159. IEEE.

[2] Abdelkader Magdy Shaaban, Christoph Schmittner, Thomas Gruber, A. Baith Mohamed, Gerald Quirchmayr, and Erich Schikuta. CloudWoT - a reference model for knowledge-based IoT solutions. In *Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services - iiWAS2018*, pages 272–281. ACM Press.

[3] ISO/IEC. Information security management systems: Overview and vocabulary. International standard, International Organization for Standardization - ISO and International Electrotechnical Commission - IEC, Geneva-Switzerland, January 2014.

[4] IEC 62443-4-2. Industrial communication networks - network and system security -part 4-2: Technical security requirements for iaas components. Technical report, International Electrotechnical Commision, 2018.

[5] Austrian Institute of Technology. Threatget - threat analysis and risk management. https://www.threatget.com. Accessed: 29.06.2019.

[6] Adam Shostack. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[7] Abdelkader Magdy Shaaban, Erwin Kristen, and Christoph Schmittner. Application of iec 62443 for iot components. In *International Conference on Computer Safety, Reliability, and Security*, pages 214–223. Springer, 2018.

[8] IEEE 1686. Ieee 1686-2013 - ieee standard for intelligent electronic devices cyber security capabilities. Technical report, Institute of Electrical and Electronics Engineers, 2013.

[9] ISA. Ansi/isa-62443-4-2-2018, security for industrial automation and control systems, part 4-2: Technical security requirements for iacs components, 2018. [accessed on: 2019.06.28].