Security Chain Tool for IoT Secure Applications

Christoph Schmittner
Austrian Institute of Technology)
Digital Safety and Security
Vienna, Austria
Christoph.Schmittner@ait.ac.at

Abdelkader Magdy Shaaban
Austrian Institute of Technology)
Digital Safety and Security
Vienna, Austria
Abdelkader.Shaaban@ait.ac.at

***Abstract*—Internet of Things (IoT) technology is a big network of machines, objects, or people interacting together to achieve a common goal. IoT domain has several security issues which are not easily detected in the earlier stages of the developing phases. This work introduces a novel security chain tool helps to identify IoT threats which exploit vulnerabilities, then determines the best security requirements which protect the IoT assets.**

***Index Terms*—IoT, IACS, Big Data, CPPS**

I. Introduction

Cyber-physical Production Systems (CPPS) consist of smart items transferring information on a global scale. They connect and build on a variety of existing technologies and components such as robotics, industrial automation and control, IoT, big data, and cloud computing [2]. IoT is considered a significant improvement for Industrial Automation Control Systems (IACS), where billions of objects, using smart data processing units are connected by the internet [5].

The IoT design is based on smart and self-configuring nodes interconnected dynamically through global network infrastructure [1]. IoT technology has been used in various domains such as smart cities, healthcare, automated driving, farming, industrial, logistics, and transportation [4].

Many security challenges resist the developing of IoT application in different domains. This work introduces a newly formed security tool for the IoT applications. Figure 1 describes the two phases of this tool. The The first phase (Left-hand side) concerns with detecting the system threats which threaten the system's information integrity, confidentiality, and integrity based on the Security Level (SL). The second phase (Right-hand side) is the security requirement management tool to cover security flaws which are detected in the first phase. This tool aims to achieve the desired security level based on the Target Security (ST).

II. Security Chain Tool

This section describes the main functionalities of the two phases in the security chain tool.

A. Threat Analysis Phase

Threat modelling phase identifies, communicates, and understand several threats. That can be applied to different IoT scenarios as automotive, railways, networks, and so on. The threat modelling tool is a plugin for Sparx System Enterprise Architect tool [6]. EA provides a basis for modelling all forms of organizational architecture, for designing and implementing new systems or developing existing ones. EA considers the best option to create the threat modelling tool. Threat modelling helps the system architect to:

- build a secure IoT application,
- Identify security vulnerabilities.
- identify threats and evaluate their risks.

This phase use threat catalogue which is created by AIT Austrian Institute of Technology. The catalogue uses several source materials to ensure a range of threats is considered. Specifically, the following source documents were used to develop the threat catalogue:

- Threat Modeling for Automotive Security Analysis [3].
- Connected cars — Threats, vulnerabilities and their impact [7].
- UN Task Force on Cyber security and OTA issues (CS/OTA).
- The ENISA, Threat Landscape 2015, Top Threats.

Figure 2 depicts a simple an automotive example using common vehicle components such as sensor, actuator, electronic control unit (ECU), and V2X Gateway. The Threat analysis tool detects all threats in the given diagram. Without any security mitigation measures the tool identifies 39 potential threats.

The tool classifies the identified potential threats into six different classes according to the STRIDE model (i.e. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (D.o.S), and Elevation of privilege). Table I summarize the numbers of the identified potential threats concerning the STRIDE model.

TABLE I
The numbers of detected potential threats according to the STRIDE model

Threat Type	Numbers
Denial of Service	5
Elevation of Privilege	5
Information Disclosure	10
Repudiation	4
Spoofing	10
Tampering	5

The tool performs a risk assessment process to classify the risk of the identified potential threats as extreme, high,

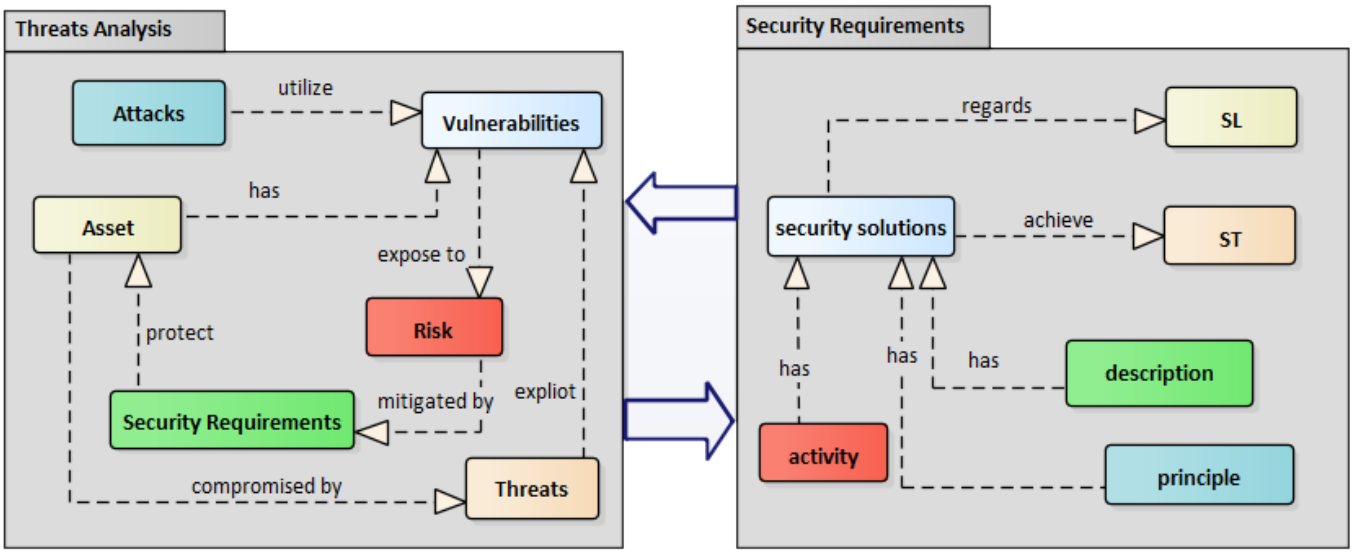

Fig. 1. Security Chain Tool

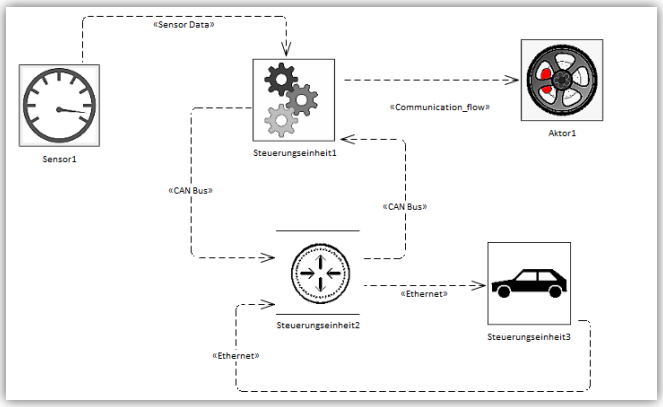

Fig. 2. IOT Automative Example

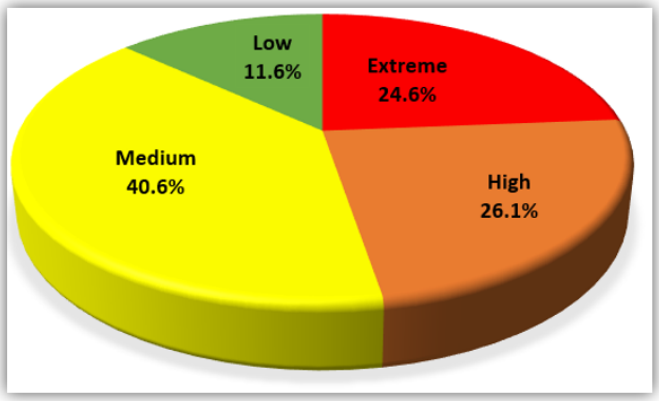

Fig. 3. Statistical percentage of risks

medium, or low risks. Figure 3 shows the statistical percentages of assessed risks of identified threats.

Afterwards, the tool aggregates all detected potential threat into one neat table to ease the traceability process as shows in figure 4.

B. Security Requirement Phase

The correct security requirement identification and efficient security requirement management are necessary for any security engineering process. We can design, and implement a secure system only if we know the exact security requirements where efficient requirement management is a challenge in system development. In the course of our research we developed the Model-based Security Requirement Management Tool (MORETO) as a tool for security requirements analysis, allocation, and management using modelling languages such as SysML/UML. MORETO is an Enterprise Architect (EA) plugin for managing the IEC 62443 security series. It is a reliable and flexible to model safety & security requirements suited to different components and system architectures. It generates a list of security requirements in a given diagram, which can help the system architect to build-up a secure infrastructure.

As mentioned earlier, ST should be defined to achieve the desired security level based on the security requirements which able to cover security issues. MORETO automatically selects suitable security requirements according to the detected threats for each component separately an illustrated in figure 5. This list shows the selected security requirements of the V2X Gateway based on the IEC 62443-4-2.

Finally, all the generated security requirements are combined into one comprehensive report which includes all details of the selected security requirements. The system architect can go through it, to check the description of each of the security requirement. Figure 6 represents a sample of the MORETO's report.

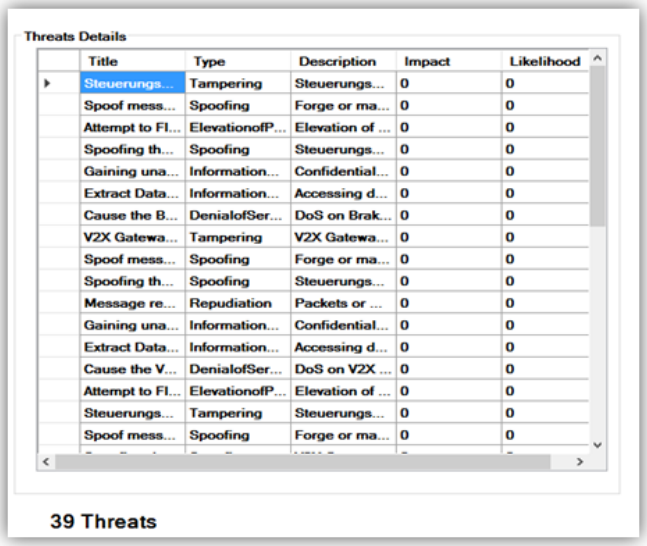

Fig. 4. List of all Indentified Threats in the Figure 2

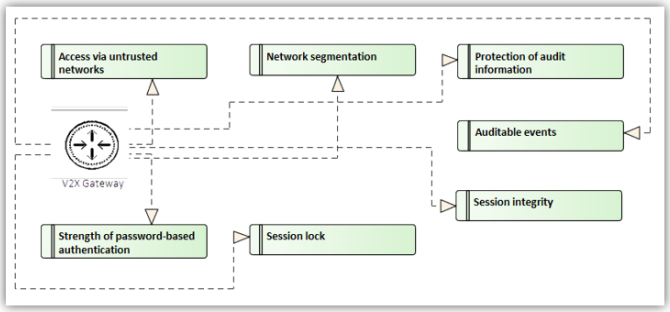

Fig. 5. Security requirements of the V2X Gateway unit

III. Conclusion

This work introduced a new security chain tool aims to deliver secure IoT applications. This work has two different phases where able to detect various types of threats and cover these identified threats by specific security requirements.

IV. Acknowledgment

This work has received funding from the iDev40 project, under grant agreement No 783163. The project is co-funded by grants from Austria, Germany, Italy, France, Portugal and ECSEL JU.

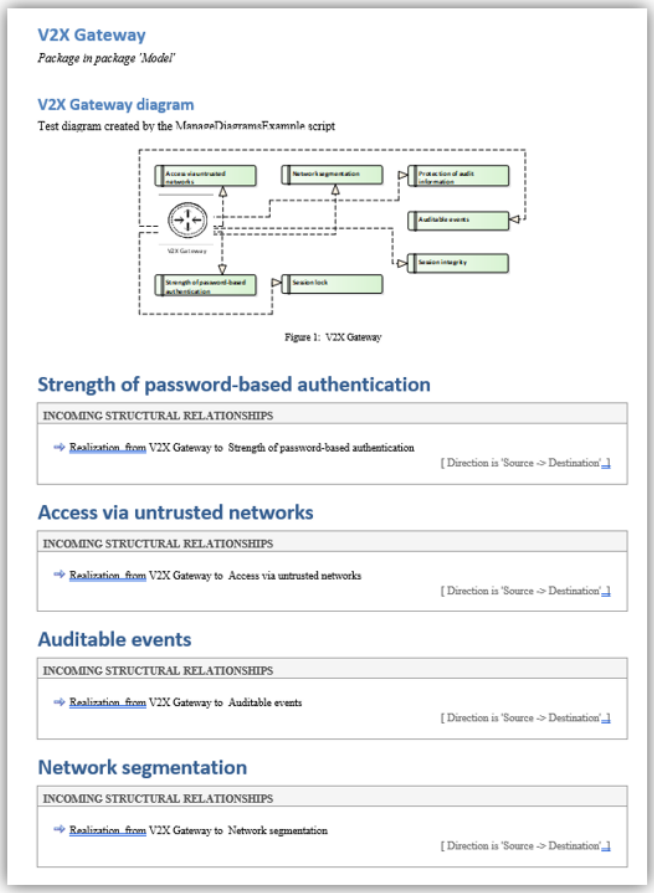

Fig. 6. Sample of MORETO report

References

[1] A. Botta, W. De Donato, V. Persico, and A. Pescapé. Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 56:684–700, 2016.

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

[3] Z. Ma and C. Schmittner. Threat modeling for automotive security analysis. 2016.

[4] H. Pei-Breivold and K. Sandström. Internet of things for industrial automation-challenges and technical. In *iThings 2015: The 8th IEEE International Conference on Internet of Things, 11-13 Dec 2015, Sydney, Australia*, pages 532–539, 2015.

[5] A. Shahzad, Y.-G. Kim, and A. Elgamoudi. Secure iot platform for industrial control systems. In *Platform Technology and Service (PlatCon), 2017 International Conference on*, pages 1–6. IEEE, 2017.

[6] SparxSystems. Enterprise architect. http://sparxsystems.com/products/ea/. Accessed: 2018-10-30.

[7] S. Strobl, D. Hofbauer, C. Schmittner, S. Maksuti, M. Tauber, and J. Delsing. Connected cars—threats, vulnerabilities and their impact. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pages 375–380. IEEE, 2018.