Automated Monitoring of Operational Technology Security and Compliance for Power Grids

Enhancing Trust by Continuous Security Configuration Monitoring

Bastian Fraune [1]

Abstract: IT security standards can increase trust in a system or component if compliance to the standard can be proven to third parties. Those standards usually specify requirements for security features, which then lead to a certain configuration of an industrial control system. Continuous monitoring of IT security configurations on intelligent electronic devices is difficult because there is no standardised way to query the security configurations of those devices. The objective of this PhD project is to enable automatic querying of security settings from industrial control system in the use case of the power grid infrastructure for remote monitoring. This opens up the possibility of automatically comparing the actual security state on the device against the defined IT security standard configurations. In such cases, industrial control systems that do not comply with defined security standards can thus be identified directly by monitoring systems in the control centre.

Keywords: ICT-Monitoring; IT-Security; OT-Security; ICS; Smart Grid; Trust; Compliance; Trusted Computing; Power Grid

1 Introduction and Motivation

Regarding the energy domain the general increase in digitization is also affecting the power grid, which is undergoing increasingly strong transition. This is characterized in particular by the restructured energy generation, which is moving from centralized generation to decentralized generation. This refers to wind turbines and wind farms, large solar farms and small solar installations on private buildings. Likewise, a variety of flexible loads and generators need to be controlled; electric cars can feed in or take out energy through their batteries and thus help to keep the physical power grid in a stable equilibrium. In order to implement such scenarios, modern communication technologies are required and inevitably the attack surfaces on the supervisory, control, and data acquisition (SCADA) systems there are increased, since (future) loads and generators can no longer communicate only via isolated communication channels.

Possible threats for the presented scenario are, for example, high-wattage botnets. In such a scenario, due to weak security configurations operational technology (OT) devices as

[1] City University of Applied Sciences Bremen, Institute of Computer Science and Automation, Flughafenallee 10, DE-28199 Bremen, Germany, bastian.fraune@hs-bremen.de

doi:10.18420/sicherheit2022_19

part of the power grid have been manipulated. After this manipulation they now operate as part of a botnet that then can be controlled remotely by the attackers. Through this hostile takeover, big loads can be manipulated and can thus be used to make profits in the electricity market [Sh21]. According to the Federal Office for Information Security Germany (BSI) security compendium, the present security issues of industrial control system (ICS) devices are, among others, insecure configuration, inadequate monitoring and detection procedures, insufficient access protection as well as inappropriate integration into organizations security [Bu21].

One general, systematic approach to counteract those general issues is to apply security measures. An international standard for information security management system is defined in the ISO 27001 series [IS17]. It describes a management process with the aim to establish and implement as well as operating and improving information security [Ke16]. To underline the importance of such standards, in Germany its application is forced by law to all operators of critical infrastructures (see §11 section 1b German „Energiewirtschaftsgesetz“[2]). On the other hand, in contrast to organisational standards, technical IT security standards describe the security requirements for OT ICS in much more concrete technical terms and defined properties. An example in the energy domain is the standard IEC 62351-7:2017 [In17]. It describes data models for network and system management and targets all network devices. Such devices shall be able to .g. detect unauthorised access, detect resource overload and detect invalid protocols.

It becomes challenging when an organisational standard is provided for monitoring the configurations, but the technical possibilities of such devices do not offer the possibility to do so. As stated in [KL15] a large portion of the critical configuration information is on the device itself, which run on proprietary or closed operating systems, which makes it more difficult to query configuration data from devices.

2 Related Work

Montesino et al. have examined the automation of information security in [MF11]. Their focus was set on the requirements of ISO 27001 and National Institute of Standards and Technolgy (NIST) SP800-53. They identified 133 security controls in annex A of ISO 27001 and 198 security control in NIST SP800-53. Two criteria were defined for the assessment of the automation capability: 1. A security control can be automated if the operation of the control can be done without human intervention, which means that it requires only machine-readable and processable resources. 2. The control can be implemented partially or completely by at least one security application. The listed security applications include, among others, Microsoft Systems Management Server, nCircle IP360 configuration and compliance server, AlienVault and PfSense Firwall. Based on the analysis, in the ISO 27001 standard 37 controls can be automated, which is 27.8% of the identified security controls.

[2] German Energy Industry Act

The analysis of the NIST SP800-53 has shown 62 controls that can be automated, making 31.3% of the 198 security controls. Despite a tabular list by category including examples, it remains unclear which controls exactly can be automated. It also looks like the settings that can be automated primarily affect the (office-) IT area.

The Security Content Automation Protocol (SCAP) is a project of NIST and emerged from the NIST IT security automation agenda. SCAP is not a protocol after all and is described on the website as "[...] a synthesis of inter operable specifications derived from community ideas"(see [Na18]). Therefore it is rather a suite of applications for exchanging security automation content, to be able to assess configuration compliance and it supports the detection of present vulnerabilities. The suite contains, among others, a vulnerability scanner, describes asset reporting formats as well as asset identification and other description languages. In 2018 NIST has announced version 2 of SCAP with a much broader focus on the overall architecture and is currently in Internet-Draft status under the Internet Engineering Task Force (IETF) as *Security Automation and Continuous Monitoring (SACM) Architecture* [WFM18]. SCAP v1 targets primarily the typical office IT domain.

Automated standard compliance for Industry 4.0 has been investigated by Bicaku et al. with the aim to express compliance in accordance to standards automatically [Bi18]. They have developed the *Monitoring and Standard Compliance Verification Framework* (MSVP), which considers security and safety standards as well as organisational indicators. For the evaluation, they queried the needed data from devices by using custom agents that are able to communicate with their monitoring system. The monitoring system then provides the collected data to their MSVP framework. The data from the devices has been collected by using custom scripts in their devices, which were located in the cloud. As data collection was not their focus, they mentioned that "[...] measurable metrics should be imposed by standardised bodies [...]"[Bi18, p. 751]. In the context of this PhD project, this underlines how important it is, to provide measurable security configurations in an integrated way.

In [Ch18] a framework for continuous compliance monitoring is presented. The authors propose a process which maps requirements from standards to an ontology and extracts the requirements from the documents using natural language processing (NLP). Their framework then links requirements with custom scripts to query data from systems. Those scripts have only been created for Powershell and demonstration purposes. It seems to be a good approach to gather information from different standards and extract requirements with NLP. Since their scripts have been made for Windows environments, they cannot be used for OT devices. But, the authors note, that it is important that the "[...] scripts have to be as atomic as possible in order to be reusable[...]". This also shows the need for a common information model that can be used to query security configuration from OT devices.

A very widely used protocol for monitoring information and communication technology (ICT) network components is the simple network management protocol (SNMP). It is standardised by RFC 3410-3418 and its original purpose was the management and configuration of network devices. Despite version 1 and 2 having security issues in their

design, it's still broadly ches and firewalls. Enhanced security was integrated in version 3, but the protocol still is mainly used for monitoring purposes [DH08].

3 Research Questions

As described, there is a gap in the ability to continuously monitor security configurations on OT devices. The associated risk is that this can lead to an unnoticed weakening of the security measures. At the same time, monitoring of configurations is mentioned as a requirement in organisational standards such as ISO 27001 [IS17]. Since the implementation of security configurations itself is a technical requirement, it should be possible to monitor them by technical means, if available [GHS17]. This is not the case for continuous monitoring of security configurations in OT devices. For this reason, this PhD project addresses the following research questions:

"How can automated monitoring of technical security configurations, for SCADA components in the energy distribution domain, be enabled?"

To be able to give an appropriate answer, sub-questions have been defined, as they allow to break the research question down and thus allow to approach it in a structured way.

Which security features are relevant from the view of existing domain standards? — It must be investigated first, which technical security requirements and features actually exist for those domains, especially OT devices in power substations. As already stated in [RU13] and [GHS17] many security standards related to smart grids exist. In order to extract the correct requirements, it is important to analyse which requirements are applicable in which context and thus necessary for this PhD project. As it is expected that typical security requirements are also included in industry standards such as the IEC 62443 series, those requirements will be considered, too.

How can existing information models from ICT component monitoring be considered? — This question aims to explore the extent, to which existing protocols for monitoring can be incorporated. The TC 57 is a technical committee of the International Electrotechnical Commission (IEC). TC 57 prepares and proposes standards for "Power systems management and associated information exchange"[In]. Many standards have been released and are currently in use. To be able to integrate the idea of the research project into the power grid, their standards have to be considered. Therefore an investigation driven by use cases is necessary in order to identify the required and applicable protocols. Suitable protocols shall be able to transport the monitoring data from the process level up to the operation and enterprise level.

The third research question is about *How can concepts of trusted computing support this?* — To enhance the trust of such monitorable security configurations an integration of hardware based trust anchors will be investigated. Trusted Computing concepts which allow to enable measured boot and remote attestation in combination with a hardware security module

(HSM) are part of the research. The HSM specified by the Trusted Computing Group (TCG) is the Trusted Platform Module 2.0 (TPM2). Such an integration into the monitoring of security configuration allows to ensure that the devices authenticity can be proven.

4 Methodology

To approach the described problem, different artefacts will be developed, which are derived from the research sub-questions. The first artefact aims at an information model suitable for querying security configurations from OT devices in the power grid. To achieve this, first the necessary or applicable security standards for the power grid are reviewed by a literature research. In the next step the needed security requirements and configurations from the identified standards are extracted. The resulting requirements then form the basis for an information model of the security configurations. In order to be able to evaluate the model, this is to be implemented iteratively on a virtual intelligent electronic device (IED). The primary development objective is the information model, that represents the required security configuration information. Thus it is the basis for further implementations and information exchange in the energy domain.

The second artefact aims to identify suitable communication protocols and extend them in order to be able to support the data from the information model. In the domain of the power grid, it must be taken into account that a large number of specific communication protocols already exist. Therefore, existing protocols are to be examined to see whether they can transmit the information model from the first artefact. Since this will probably not be the case, the most suitable protocol should be identified and then enabled to do so. The implementation is first carried out by analysing the capabilities of the communication standards of the TC 57 Group. The focus will be on the communication protocols between the sub-station and the control centre. The evaluation of those protocols will be done against the information model from the first artefact. A prototypical implementation will be used to represent a continuous evaluation of the research.

5 Conclusion

In order to get closer to a possible solution for the outlined research question, the primary research question and derived sub-questions were presented, as well the methodology to approach a solution. The answers to these questions should lead to the objective of automated verification of security configurations of OT devices. With such new possibilities, security audits for compliance and automated monitoring of OT devices can be enabled. Automatic proof of compliance with relevant security standards also contributes to increase trust in the system or the queried device. In the next steps, the use cases will be defined more precisely and more in-depth in order to be able to address the research questions in a more targeted way.

Bibliography

[Bi18] Bicaku, Ani; Schmittner, Christoph; Tauber, Markus; Delsing, Jerker: Monitoring Industry 4.0 applications for security and safety standard compliance. In: 2018 IEEE Industrial Cyber-Physical Systems (ICPS). IEEE, pp. 749–754, 2018.

[Bu21] Bundesamt für Sicherheit in der Informationstechnik (BSI): , IT-Grundschutz-Kompendium, 2021.

[Ch18] Cheng, Danny C.; B., Jod; Cu, Gregory; Rose, Nathalie: Towards end-to-end Continuous Monitoring of Compliance Status Across Multiple Requirements. International Journal of Advanced Computer Science and Applications, 9(12):456–466, 2018.

[DH08] Dinger, Jochen; Hartenstein, Hannes: Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung. Universitätsverlag Karlsruhe, 2008.

[GHS17] Genzel, Carl-Heinz; Hoffmann, Olav; Sethmann, Richard: Zusammenfassung relevanter Informationssicherheitsstandards für deutsche Verteilungsnetzbetreiber. Technical report, Hochschule Bremen - FRI, 2017.

[In] International Electrotechnical Commission (IEC): , IEC - TC 57 Scope.

[In17] International Electrotechnical Commission: , Power Systems Management And Associated Information Exchange - Data And Communications Security – Part 7: Network And System Management (NSM) Data Object Models (IEC 62351-7:2017) (English Version), 2017.

[IS17] ISO Central Secretary: Information technology - Security techniques - Information security management systems - Requirements. Standard ISO/IEC 27001:2017, International Organization for Standardization, Geneva, CH, 2017.

[Ke16] Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen; Schröder, Klaus-Werner: IT-Sicherheitsmanagement nach der neuen ISO 27001. Springer Fachmedien Wiesbaden, Wiesbaden, 2016.

[KL15] Knapp, Eric D.; Langill, Joel Thomas: Security Monitoring of Industrial Control Systems. In: Industrial Network Security, pp. 351–386. Elsevier, 2015.

[MF11] Montesino, Raydel; Fenz, Stefan: Information Security Automation: How Far Can We Go? In: 2011 Sixth International Conference on Availability, Reliability and Security. IEEE, pp. 280–285, aug 2011.

[Na18] National Institute of Standardization and Technology (NIST): , Security Content Automation Protocol - Project Overview, 2018.

[RU13] Rosinger, Christine; Uslar, Mathias: Smart Grid Security: IEC 62351 and Other Relevant Standards. In: Power Systems, volume 71 of Power Systems, pp. 129–146. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[Sh21] Shekari, Tohid; Irvene, Celine; Cardenas, Alvaro A.; Beyah, Raheem: MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. ACM, New York, NY, USA, pp. 1338–1356, nov 2021.

[WFM18] Waltermire, David; Fitzgerald-McKay, Jessica: Transitioning to the Security Content Automation Protocol (SCAP) Version 2. Technical report, National Institute of Standards and Technology, Gaithersburg, MD, Sep 2018.