Automated Security Analysis for Industrial Control Systems based on MITRE ATT&CK and IEC 62443

Jonas Vogl

KASTEL
Institute for Anthropomatics
Karlsruhe Institute of Technology (KIT), Germany
Jonas.Vogl@kit.edu

Abstract

In this article a lightweight approach to automatically analyze the architecture of Industrial Control Systems (ICS) for cybersecurity issues is presented. The goal is to support network architects and administrators with identifying security weaknesses in their network architecture and help them find efficient solutions. For this a mapping between the attacker focused MITRE ATT&CK Framework [9] and the defense oriented IEC 62443 standard [5] is created. This mapping is then used to estimate for which attack techniques defenses are already in place or have to be improved.

1 Introduction

To set up an effective and efficient defense, it is vital to have good information on the assets and systems that have to be defended as well as the attacker. This is no new concept to the cybersecurity community and there are numerous projects that collect security relevant data. For this article mainly two of those projects are relevant. The MITRE ATT&CK Framework [9] is a collection of empirical data of attack behavior, which is used to model attackers in this work. The IEC

62443 standard [5] contains a collection of mitigations and recommendations when to employ them. IEC 62443 is used here to model the system under consideration (SUC). Besides that there are the Common Vulnerabilities and Exposures (CVE) [2] and Common Weakness Enumeration (CWE) [3] databases and several security standards that collect security best practices.

While there are many sources of information about many different aspects of cyber security, they tend to have their own focus. Many can be categorized as either attacker focused (CVE, CWE, MITRE ATT&CK) or defender focused (standards such as 62443, NIST CSF[11]). Combining these different sources is potentially valuable for security, but also tedious. There are several different works from recent years that map different databases frameworks and standards [7, 4, 8].

Another observation about especially the attacker centric databases is that they focus on finding and collecting vulnerabilities. Finding and closing vulnerabilities is an essential part of cyber security. However it forces the defender into a reactionary role where the defender waits for new vulnerabilities to be found and then close them. More proactive methods that can help improve a systems security without relying on knowledge of new vulnerabilities would be a good addition to defensive tools available. Other work in this direction is for example MITRE's Infrastructure Susceptibility Analysis and Assessment [10] project which is an attempt to forecast attacker behavior. It is in an early stage with no published results yet though.

This article contributes to the ongoing effort to better link and use the different existing knowledge bases by proposing a method to automatically analyze a system's security without relying on known vulnerabilities. A mapping of mitigations standardized in 62443 to the attack techniques collected in the MITRE ATT&CK framework is used to find weaknesses in a system's security concept based on the security requirements found in that system's risk assessment.

1.1 IEC 62443

IEC 62443 Security for Industrial Automation and Control Systems [5] is a collection of standards that codifies best practice knowledge specifically for

cybersecurity of ICS. While it's different parts are intended for different actors like device manufacturer, system owner/operator or integrator, IEC 62443's focus is on defense. Depending on the level of security required 62443 specifies mitigations that have to be implemented. While 62443 specifies what has to be done, it does not specify how. That means 62443's requirements can be met not only by technical measures, physical measures or policies such as fences or restrictions on the use of private devices are equally valid as well.

For this work we focus on 62443-3-3 of the standard, which describes security measures that are used to protect systems [6]. It is targeted towards operators and integrators of ICS and specifies which mitigations have to be implemented to achieve a given Security Level.

Security Levels in 62443. In 62443-3-3 mitigations are tied to Security Levels (SL). As the Security Level increases, 62443-3-3 specifies additional mitigations to defend against stronger attackers, that are associated with the higher Security Level. An overview of the 4 different security levels in 62443 can be found in Table 1.1. The main characteristic of each SL that differentiates it from the other SLs is highlighted in italic. SL 1, the lowest security level protects only against random events such as random bitflips that can happen on any carrier or natural disasters. So SL 1 is mostly concerned with safety, not security. From SL 2 on intelligent attackers of low motivation and skill are considered. Starting with SL 3 it is assumed attackers have ICS specific knowledge, which allows for more sophisticated attacks. On the highest Security Level, SL 4, Advanced Persistent Threats (APT) such as criminal organisations or government agencies are considered. They have significantly higher motivation and resources compared to other attackers.

Requirements in 62443-3-3. Part 3-3 of IEC 62443 specifies the requirements that have to be implemented in an ICS network to achieve a given security level. These are mitigations, organized in Foundational Requirements (FR), System Requirements (SR) and Requirement Enhancements (RE).

Foundational Requirements (FR) are broader categories that group SRs together based on the security goal they are supposed to achieve. Examples for FRs are Use Control, System Integrity or Restricted Data flow.

Security Level	Threat Type	Attacker Motivation	Attacker Skill
SL 1	*Unintentional*	None	None
SL 2	*Intentional*	Low	Low
SL 3	Intentional	Moderate	*ICS Specific*
SL 4	Intentional	*High*	ICS Specific

Table 1.1: Security Levels in IEC 62443

System Requirements (SR) are the base mitigations that can be implemented in an ICS network. Each SR is assigned a Security Level, usually SL 1 or 2. To achieve a Security Level all assigned SRs have to be implemented. Examples of SRs are authorization enforcement for all human users, auditable events or session locks. All three examples are assigned to FR 2 Use Control.

Requirement Enhancements (RE) are additional mitigations that improve on a given SR. They are also assigned Security Levels. Usually they are required to increase the SL of a SR to higher SLs of 3 or 4. As an example consider the enhacements to SR 2.1 authorization enforcement for human users, which is required from SL 1 on. To increase the SL to 2 the REs authorization enforcement for all users and a role that can assign permissions have to be implemented. To increase SL further supervisor override (SL3) and dual approval (SL4) need to be added.

Mitigations in 62443 are not all aimed at preventing an attack, but also at detecting an attack and recovering from it.

1.2 MITRE ATT&CK Framework

The MITRE ATT&CK framework [9]is a large knowledge base in which attacker behaviour is collected. The structure and design goals of the MITRE ATT&CK framework is explained in [1] [12].

The framework is structured into tactics, techniques and procedures. Tactics represent the different goals an attacker might have to achieve for a successful attack such as initial access, defense evasion, or impact. Not every attack has

to achieve all tactics. For each tactics there exist several different techniques attackers use to achieve the tactic. Some example techniques that belong to the impact tactic are Denial of View, Loss of Control or Damage to Property. While a tactic represents what an attacker wants to achieve, the techniques are how an attacker can achieve the tactic.

The third part of the MITRE ATT&CK structure is the procedure. Procedures represent the implementations of techniques. So for each technique there can be several procedures. Procedures are what is observed ”in the wild”, tactics and techniques are abstractions of that to better understand the attacker intent behind the procedure and to categorize them.

2 Automated Security Analysis

Here a concept for automated security analysis is presented. It consists of three parts, the system under consideration (SUC), the attacker model and the analysis method. The SUC is modeled in terms of mitigations that haven been deployed, as IEC 62443 describes them. The attacker model consists of a list of MITRE Techniques. The final component is the mapping of IEC 62443 and MITRE ATT&CK that ties attacker model and SUC together. All three parts are described in more detail below.

System Under Consideration. The SUC is modeled in terms of the mitigations that are implemented, as they are described in IEC 62443. All information required about the SUC for this analysis is a list of the SR/RE that are implemented in the SUC. While this SUC lacks technical details because of its abstraction, this also allows proactive scanning, without knowledge of vulnerabilities in the system. This also allows to factor in non-technical mitigations.

Attack Model. For the attacker model we use MITRE ATT&CK Techniques. Techniques are on a level of abstraction similar to that of 62443s SRs. An attack is represented by a list of all techniques used in the attack.

Mapping MITRE techniques to 62443. To analyze the threat a set of MITRE Techniques poses to a SUC, a connection between mitigations and attack techniques is required. For this a mapping between MITRE Techniques and SR/REs

is created. Each pair of technique and mitigation (SR/RE) can have one of two types of relationships. A technique can either *circumvent* a mitigation or a mitigation *mitigates* a technique. For example the technique deobfuscation (T1140) **circumvents** the RE ”Malicious code protection on entry and exit nodes” by hiding malicious code in seemingly innocent files. On the other hand the deobfuscation technique can be **mitigated** by ”Zone boundary protection” (SR 5.2). It is also possible that a pair of technique and SR/RE does not directly influence each other. Note that this mapping does not represent guarantees that a circumvention or mitigation is always successful but rather that a circumvention or mitigation is likely.

The resulting mapping can be thought of as the rules for a game of Rock, Paper, Scissors, where a technique wins (circumventing them) against some SR/REs while loosing to others (being mitigated by them). This mapping can then be used to compare a given system against an attack (a list of techniques) to find out if mitigations against the attack are in place or if defenses are lacking.

2.1 Usage

This analysis relies on an already conducted risk assessment. Guidance on how to conduct a risk assessment can be found for example in IEC 62443-3-2 [5]. During a risk assessment, already deployed security measures are identified as well as relevant attacks. This information can then feed the security analysis proposed here. Relevant attacks then have to be described as collection of MITRE techniques. And if the risk assessment was not already done according to 62443 some additional work is necessary to translate mitigations to SR/REs. Overall the overhead of using this approach is low, since all information required is collected during a risk assessment process anyways.

By comparing the lists of implemented SR/REs against relevant techniques it is possible to estimate whether an attack is already reasonably mitigated or requires more mitigations against it. The mapping as well as the mitigations in MITRE associated with a technique can be used as guidance on how to improve security.

3 Outlook

In this article a method to proactively analyze security of ICS systems was presented. It uses relatively abstract information about both attacks and SUC. This makes the method easy and cheap to employ. But that also means that results are abstract and ignore some factors. This abstraction allows this method to be used proactively, without taking vulnerabilities into account. After this initial method is implemented and evaluated in a lab environment it will be enhanced by adding information and missing factors to the models, depending on the results of the evaluation. Some missing factors that can be added are more details about SUC, such as network architecture, devices and vulnerabilities. On the attacker side it might be useful to also take into account in which order different tactics have to be achieved for a successful attack.

Other recent works, such as those of Kuppa et.al. [7], Grigorescu et.al. [4] or Kwon et.al. [8] map MITRE to other cybersecurity resources such as the CVE database or the NIST Cybersecurity framework. MITRE's Infrastructure Susceptibility Analysis and Assessment [10] also attempts to improve to use security information predictively. So this work falls into a recent effort of different actors to improve the usage of security information leveraging MITRE.

References

[1] Blake E. Strom et al. *ATTACK Design and Philosophy March 2020 Revision*.

[2] CVE. *Common Vulnerabilities and Exposures*. URL: https://www.cve.org/.

[3] CWE. *Common Weakness Enumeration*. URL: https://cwe.mitre.org/.

[4] Octavian Grigorescu et al. "CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques". In: *Algorithms* 15.9 (2022). ISSN: 1999-4893. DOI: 10.3390/a15090314. URL: https://www.mdpi.com/1999-4893/15/9/314.

[5] ISA. *ISA-62443 Security for Industrial Automation and Control Systems*.

[6] ISA. *ISA-62443-3-3 Part 3-3: System security requirements and security levels*.

[7] Aditya Kuppa, Lamine Aouad, and Nhien-An Le-Khac. "Linking CVE's to MITRE ATT&CK Techniques". In: *Proceedings of the 16th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, 8172021, pp. 1–12. ISBN: 9781450390514. DOI: 10.1145/3465481.3465758.

[8] Roger Kwon et al. "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping". In: *2020 Resilience Week (RWS)*. 2020, pp. 106–112. DOI: 10.1109/RWS50334.2020.9241271.

[9] MITRE. *MITRE ATT&CK Framework*. URL: https://attack.mitre.org/.

[10] MITRE. *MITRE Infrastructure Susceptibility Analysis and Assessment*. URL: https://www.mitre.org/news-insights/fact-sheet/infrastructure-susceptibility-analysis-and-assessments.

[11] NIST. *Framework for Improving Critical Infrastructure Cybersecurity*.

[12] Otis Alexander, Misha Belisle, and Jacob Steele. *ATTACK for ICS - Design and Philosophy*.