Analysis of and Mitigation Strategies for Real World ICS Security Incidents

Nico Fechtner

Technical University of Munich &
Fraunhofer Institute for Applied and Integrated Security
nico.fechtner@tum.de

Abstract. As more and more Industrial Control Systems (ICS) are getting connected to the internet and IT networks—intentionally or by mistake—the attack surface of these systems increases dramatically. Due to this, the number of real world ICS security incidents rises, too, which is why it is crucial to develop efficient detection and mitigation strategies. A solid baseline in this process is analyzing and learning from past incidents. This is crucial to avoid common mistakes and to effectively prevent future incidents. To aid this process, this paper proposes a systematic comparative overview of historic ICS security incidents focussing on various parameters including targets, threat actors, attack techniques, goals and impacts, dwell times, operator reactions and detection and mitigation strategies. Several key findings are resulting from this overview and an in-depth analysis of the Triton incident. First, x. Second, y. Third, z.

Keywords: ICS Security · Security Incident · Triton.

1 Introduction

While Information Technology (IT) refers to software and hardware that generate data for enterprise use, Operational Technology (OT) describes software and hardware able to detect or cause a physical event in an industrial environment. Probably the most important subcategory of OT, at least revenue-wise, are Industrial Control Systems (ICS). They are used in a wide variety of industries such as food and agriculture, energy, water, transportation, chemical, nuclear power, pharmaceutical and discrete manufacturing [6].

Initially, ICS were not connected to the internet and strictly separated from IT networks. Due to this isolation, it was hard if not impossible for adversaries to remotely attack ICS which is why until recently security was not a big concern to companies running ICS. Instead, they traditionally focus on safety, continuity and efficiency of their systems. However, the attack surface of many ICS changed within the last two decades since they got connected to traditional IT networks and the internet—sometimes intentionally, sometimes by mistake. Inevitably, this led to an ongoing series of ICS security incidents.

While more and more of those incidents are reported, it is business-critical to develop suitable detection and mitigation strategies. A solid baseline in this process is analyzing and learning from past incidents. This is crucial to avoid common mistakes and to effectively prevent future incidents. To aid this process, this paper proposes a systematic comparative overview of historic ICS security incidents focussing on various parameters including targets, threat actors, attack techniques, goals and impacts, dwell times, operator reactions and detection and mitigation strategies. The overview aims at identifying common attack patterns that could be used to prevent future attacks. To the best of the author's knowledge, such an overview has not yet been published.

In addition, the Triton incident of 2017 will be analyzed in detail to showcase how attackers perform sophisticated ICS attacks and which detection and mitigation strategies can be derived from their methodologies. The incident was chosen due to its potential life-threatening impact and the novel attack approach targeting Safety Instrumented Systems (SIS).

The remainder of the paper is structured as follows. Section 2 provides an overview of related work in the area of ICS incidents which is used as the basis of the comparative overview that is provided in Section 3. Exemplary the Triton incident is analyzed in detail in Section 4. Section 5 concludes the paper by emphasizing the need to learn from past mistakes.

2 Related Work

There are four main types of publicly available sources that provide information on ICS security incidents. First, there are incident enumerations like the Risi Database[1] and the ICS-CERT Alerts[2]. On the one hand, the fact that those repositories aim to aggregate all observed ICS incidents from around the world makes them useful for getting a high-level overview of the current threat landscape. On the other hand, however, they only provide basic information about the incidents and do not analyze them in detail. Second, ICS security companies like Dragos [4] and CyberX [2] publish yearly ICS threat reports discussing relevant incidents. Those reports are neither complete with regards to the incidents they cover nor do they provide in-depth analyses of the covered attacks. However, they do a good job of highlighting trends in the threat landscape throughout the years. Third, there are dedicated scientific papers focussing on single ICS incidents like the attacks targeting the Ukraine power grid [1] or the Triton malware [3]. Those papers usually cover single incidents in-depth and help in understanding how exactly the adversaries operated. Fourth, there are numerous blog posts, press releases and conference talks covering ICS incidents. In addition, there is already a paper proposing an overview of historical ICS security incidents [5]. However, the paper is slightly dated and, more importantly, does not compare the different incidents systematically. All of the above-mentioned sources are taken into account to achieve exactly this in the upcoming section.

[1] https://www.risidata.com/Database

[2] https://www.us-cert.gov/ics/alerts

3 Comparative Overview of ICS Security Incidents

From the resources and literature stated in Section 2, a total of 30 ICS security incidents were extracted. Those form the basis of the following analysis and can be found in table [appendix table]. In the subsections below, a comparative overview of these incidents will be given. Each subsection tries to compare the incidents with regards to specific attributes, e.g. the involved threat actors or the utilized attack techniques. Most subsections contain both quantitative as well as qualitative analyses. Please keep in mind, though, that the quantitative analyses are solely intended to highlight important trends and that the according absolute values might contains inaccuracies. This is due to the fact that often specific information about incidents is unknown. For example, consider the dwell time which describes how long an adversary is in a system before the actual attack payload is executed. Sometimes it is possible to give an accurate estimation for this number thanks to digital forensics after an incident. In general, however, this is a non-trivial task and even if performed successfully, it may still lead to incorrect conclusions about the dwell time and other incident attributes.

3.1 Targets

3.2 Threat Actors

3.3 Attack Techniques

3.4 Attack Goals and Realized Impacts

3.5 Dwell Times and Reactions

3.6 Detection and Mitigation Strategies

4 Detailed Analysis of the Triton Attack

4.1 The Petro Rabigh Oil Refinery

4.2 The Attackers' Approach

4.3 Impact

4.4 Attribution

4.5 Detection and Mitigation Opportunities

5 Conclusion

References

1. Case, D.U.: Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC) **388** (2016)
2. CyberX: 2020 global iot/ics risk report (2020)

3. Di Pinto, A.A., Dragoni, Y., Carcano, A.: Triton: The first ics cyber attack on safety instrument systems. In: Proc. Black Hat USA. pp. 1–26 (2018)
4. Dragos: 2019 - year in review: The ics landcape and threat activity groups (2020)
5. Hemsley, K.E., Fisher, E., et al.: History of industrial control system cyber incidents. Tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States) (2018)
6. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ics) security. NIST special publication **800**(82), 16–16 (2011)