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 [8].

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 literature and resources stated in Section 2, a total of 29 ICS security incidents were extracted. Those form the basis of the following analysis and can be found in table [appendix table]. Note that due to incidents not being reported, the tremendous amount of incidents that are reported and new incidents occurring steadily, this table is inherently incomplete, but rather tries to focus on the most prevalent attacks launched until February 2020. 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.

3.1 Targets

When analyzing the entities affected by ICS security incidents there are two fundamentally different kinds of attacks that have to be considered separately. On the one hand, there are targeted attacks against unique entities. Making up roughly 86% of the analyzed incidents, targeted attacks seem to present a diverse threat landscape to ICS and will therefore be analyzed in detail below. On the other hand, there are untargeted attacks. Here, the threat actors are not interested in the specific entities that will be affected by the attack, but rather they aim for as many incidents as possible. Often this is achieved by a self-replicating component within the malware used for the attacks. While only four of the analyzed incidents fall into this category, they still pose a significant threat to ICS. Interesting to see is that the malware used for untargeted attacks usually is not tailored specifically for ICS environments, but rather targets common operating systems like Microsoft Windows and enterprise networks in general. Many instances of untargeted attacks fall in the category of ransomware. For example, the popular WannaCry ransomware spread not only to desktop computers around the world but also infected a series of ICS workstations e.g. at a Taiwanese manufacturing plant leading to outages due to encrypted hard drives [7]. This kind of incidental infections of ICS systems with malware originally intended for enterprise networks are becoming more and more of a threat in recent years [4], [2], [10].

Since untargeted attacks are not aimed at specific entities but often solely intend to infect as many systems as possible, e.g. with self-replicating components, there is in general no pattern observable in terms of the geographical location or the economic sector of the affected parties. Targeted attacks, however, can be analyzed for such patterns.

When it comes to the geographical location of ICS attack victims, the areas most often affected seem to be the Middle East and Europe. The Middle East is being targeted by about 56% of the analyzed attacks. Especially companies located in Saudi Arabia often fall victim to attacks. Probably the most well-known incident taking place there was Triton which targeted a Saudi Arabian petrochemical plant and will be covered in depth in Section 4. Companies located in Europe are targeted by about 52% of the analyzed attacks. The country affected the most until now is Ukraine falling victim to multiple attacks targeting its power grid. In about 24% of the analyzed incidents, the US were amongst the victims. Interesting is that while being home to important global threat actors as discussed in Subsection 3.2, neither Russia nor China nor North Korea reports a lot of ICS incidents against entities located in their countries. However, this does not necessarily mean that no ICS incidents occur in these countries, but it could also be the case that incidents are just not as liberally published as by other countries. Especially China and North Korea are known for withholding most of the cyber attacks taking place in their country [citation].

When it comes to the economic sector falling victim to targeted ICS attacks, the most affected one is the energy sector being targeted in about 52% of the analyzed targeted attacks. Most and foremost, those operations include attacks against power grids like the attacks taking place in 2014 and 2015 in Ukraine. Other examples of targeted entities within the energy sector include oil and gas pipelines and refineries. The remaining victims of ICS attacks are spread across a wide variety of other economic sectors including manufacturing, water, petrochemical, governmental organizations and transportation.

3.2 Threat Actors

In total, 16 specific threat actors were involved in the analyzed ICS incidents according to the current state of research. Note, that there are often multiple names for a single threat group. They originate from different ICS security agencies and companies [9] and can be used interchangeably. This paper tries to use to the most commonly used names regardless of which entity coined it.

When it comes to the threat actors responsible for ICS attacks there is the fundamental issue of attribution. Most often, threat actors want to stay anonymous and do not confess performed attacks. Therefore, there are often only conjectures about the threat actors involved in certain attacks. In line with that, 38% of the analyzed attacks cannot be associated with a specific threat actor. Furthermore, it is often difficult to locate threat actors geographically, since they usually apply various techniques to hide their physical location [6]. With regards to the analyzed incidents, 38% of the threat groups cannot be associated with a specific country. It can be said, however, that 28% of all analyzed attacks are known to originate from Russia and 24% are known to originate from the Middle East, thereof 71% from Iran. Other countries being home to important threat groups are China, the US and North Korea. The most active threat actors according to the sample of incidents taken into account here, are Energetic Bear from Russia, being involved in 14% of all attacks, and APT33 from Iran, being involved in 10% of all attacks. Interesting to note is, that some threat groups primarily act on their own while others collaborate with each other. For example, APT33 often collaborates with other Iranian threat groups, whereas Energetic Bear mostly acts alone. When it comes to the team size, only one threat actor is an individual person, all others are groups comprised of multiple people. This person, Vitak Boden, performed what can be considered one of the first ICS attacks ever. To take revenge on a wastewater facility where he was rejected when applying for a

job, he manipulated the sewage pumping stations via an RF transmitter which lead to millions of gallons of untreated sewage water being released into waterways and local parks [5]. Since this incident in the year 2000, ICS attacks got a lot more sophisticated which is why the team size of threat groups continues to grow.
72% of the analyzed attacks are considered to be performed by government-funded threat actors. On the one hand, targeted ICS attacks require a large amount of knowledge and resources which often only nation-states can provide. On the other hand, governments can profit in various ways from ICS attacks against foreign countries, be it through industrial espionage, by making critical facilities and infrastructures unavailable or even by targetting human lives. Often ICS attacks can be seen as an act of war.

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. Huang, K., Siegel, M., Madnick, S.: Systematically understanding the cyber attack business: A survey. ACM Computing Surveys (CSUR) **51**(4), 1–36 (2018)
7. Skybox Security Inc.: Tsmc wannacry hits ot plants with a hefty price tag. https://blog.skyboxsecurity.com/tsmc-wannacry/ (2018), [Online; accessed 27-April-2020]
8. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ics) security. NIST special publication **800**(82), 16–16 (2011)
9. ThaiCERT: Threat groups cardss: A threat actor encyclopedia (2019)
10. Zimba, A., Wang, Z., Chen, H.: Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. Ict Express **4**(1), 14–18 (2018)