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. The abstract should briefly summarize the contents of the paper in 150–200 words. The goal is to communicate: Background/motivation/context, Aim/objective(s)/problem statement, Approach/method(s)/procedure(s), Results, Conclusion(s)/implications.

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 [1].
Initially, ICS were not connected to the internet and strictly separated from IT networks. Due to this isolation, it was hard 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 and 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 was not yet 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 this process. 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

3 Comparative Overview of ICS Security Incidents

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. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ics) security. NIST special publication **800**(82), 16–16 (2011)