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 [14].
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 [7] and CyberX [5] 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, dedicated scientific papers are focussing on single ICS incidents like the attacks targeting the Ukraine power grid [4] or the Triton malware [6]. 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 the MITRE ATT&CK ICS database[3] which includes information on tactics, techniques, and software used by threat groups to perform ICS attacks. Furthermore, there is a paper proposing an overview of historical ICS security incidents [10]. However, it is slightly dated and, more importantly, does not compare the

[1] https://www.risidata.com/Database
[2] https://www.us-cert.gov/ics/alerts
[3] https://collaborate.mitre.org/attackics/index.php/Main_Page

different incidents systematically. All of the above-mentioned sources are taken into account to achieve exactly this in the upcoming section.

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 [13]. 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 [7], [5], [16].
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 [15] 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 [11]. 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 [10]. 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

An established model to characterize ICS attacks is the ICS Cyber Kill Chain developed by the SANS institute and depicted in figure 1. It is comprised of two stages. In stage one, IT intrusion preparation and execution takes places, i.e. the attacker compromises the IT network and positions herself in the ICS network. This stage can be completed without specific knowledge about ICS technologies or protocols. In stage two, ICS attack development and execution are performed, e.g. an attack targetting certain actuators—for example, water pumps—is developed, tested, and executed.

When it comes to the initial access in stage one of the ICS Cyber Kill Chain, two attack techniques seem to be most popular among the analyzed incidents. The first one is spearphishing which was reportedly performed in at least 26% of the attacks. The second one are zero day exploits which were utilized in at least 11% of the attacks. When inside the victims IT network, attackers often use common software. For example, in at least 11% of the cases Mimikatz was used for credential capturing. Often, popular exploitation frameworks like Metasploit and Cobalt Strike are used, too. More recent trends are the use of sophisticated obfuscation and evasion techniques and *living off the land* tools—like PowerShell or PsExec—in order to avoid being detected by Intrusion Detection Systems (IDS).

Since the core of untargeted attacks is usually ransom- or wiperware, they do not go beyond stage one of the ICS Cyber Kill Chain. Targeted attacks, however, aim more and more often to exploit the ICS environment, which requires the attackers to first gain access to the ICS network. One possible way to pivot is lateral movement via Windows authentication services. Once in the ICS network, a multitude of different exploit strategies has been reported. Most adversaries attack

ICS components like Programmable Logic Controllers (PLCs) or Safety Instrumented Systems (SIS) to modify their behaviour or to make them fail altogether. Doing so, they are often able to control actuators like waterpumps, fake the values of sensors or turn off the power supply. To make disaster recovery harder, attackers often wipe Human-Machine Interfaces (HMIs), too. While according to the ICS Cyber Kill Chain stage one typically has to take place before stage two, there is an example where the attack was performed the other way around. In 2013, an unknown attacker stole login credentials of a third-party heating, ventilation, and air conditioning (HVAC) contractor of US Target Stores. From the ICS network she then pivoted into the IT network in order to install credit card stealing software. [10]
One important trend in addition to the techniques described above is the trend away from highly manual attacks specifically tailored for a single victim towards more victim-agnostic ICS attack frameworks enabling scalable attacks. A case in point are the attacks on the Ukraine power grid. The first attack in 2015 was highly manual and the effort put into it could not be directly utilized for attacks against other energy infrastructures. One year later, however, there was a second attack targeting the power grid, but this time the adversaries had developed a framework which in theory allows them to scale their attack to a multitude of different victims with a relatively small effort. [1]

3.4 Attack Goals and Realized Impacts

The most common goal of adversaries is to extract data from the victim's systems. 37% of all analyzed attacks were designed to achieve exactly this. Other goals often persued by attackers are to cause disruption (22%), to provoke a ransom payment (15%), and to cause physical damage (11%).
When it comes to the underlying motivations of attackers, three distinct ones seem to dominate. First, attackers often strive for monetary gain. This motivates ransomware attacks like WannaCry or LockerGoga as well as information stealing with the goal of selling the data to the highest bidder. Second, some adversaries are interested in the data they steal themselfs and do not intend to sell them. This motivates ICS espionage operations like StoneDrill were Iranian threat groups gathered intelligence about Saudi Arabian ICS environments. Third, there are threat actors which intend to disrupt the regular operation of ICS by causing outages or even physical damage. The latter was e.g. the case in the famous Stuxnet incident in 2010 were the US and Israelian government attacked nuklear enrichment facilities of Iran in order to sabotage the possible development of nuklear weapons. Untargeted attacks falling into this category are typically related to wiperware which erases or encrypts hard drives without a subsequent ransom demand.
In total, a minimum of 85% of the attacks are considered to be at least partly successful in achieving their goals with regards to some of their victims. Typical impacts include information loss, financial loss—via physical damage, ransom payment or costly recovery processes—and environmental damages. Fortunately, until to date, there are no ICS incidents known which killed humans.

One incident considered to be unsuccessful is the well-known Triton attack which failed for reasons not fully understood up until today. Section 4 will provide a detailed analysis of the incident and its impacts. Furthermore, untargeted attacks often partly fail to achieve their goal since a lot of companies can restore operations without a long outage or paying a ransom thanks to sufficient backup strategies.

3.5 Dwell Times and Reactions

Dwell time describes how long an adversary is in a system before the actual attack payload is executed. While sometimes it is possible to give an accurate estimation for this number thanks to digital forensics after an incident, keep in mind that, in general, this is a non-trivial task and potentially leads to inaccuracies. A rough trend, however, can be detected when analyzing important ICS incidents. In the context of untargeted attacks, the dwell time usually is a matter of days, while when speaking about targeted attacks, the dwell time typically ranges from multiple months, e.g. in the attacks targetting the Ukraine power grid and the Triton incident, to multiple years. The latter is considered to be the case, for example, when considering the Red October espionage campaign against multiple countries initiated by a Russian threat actor. It seems that with dwell times this long it should be possible for the ICS network operators to detect that something is wrong within their systems before the adversaries deliver the final payload. Unfortunately, while this holds true in theory, attacks usually are not detected in their early stages in practice. There are some cases—BlackEnergy and Triton—where the administrators were able to detect that something is wrong before the actual attack payload was executed, but most often only after the final exploit is delivered the attack is detected.
When it comes to reacting to an untargeted attack, there is sometimes the option to pay a ransom in order to get the hard drives decrypted again by the adversary. While this should be avoided, since there is no certainty that the attackers will indeed decrypt the hard drives as promised, there are still cases known were the ransom was payed. Often companies have dedicated insurances that cover such ransom demands under certain circumstances. The typical response to a destructive untargeted attack, however, is to restore operations from backups. In the case of targeted attacks, when operators suspect that an intrusion has happened, they often shut down the ICS in order to prevent further breaches, physical damage, and threats to human lifes. This happened, e.g. in the Triton incident. When the final payload was already delivered by the adversaries, however, often the only thing left to do is to start recovery processes that aim to restore operations and typically also include digital forensics in order to analyze how the incident could have happened, e.g. how the ICS network could be breached, in the first place.

3.6 Detection and Mitigation Strategies

After comparatively analyzing 28 ICS incidents a multitude of possible detection, and mitigation strategies can be identified which can be leveraged to defend ICS against future threats.
To be able to detect ongoing ICS attacks, the first fundamental resource is an up-to-date asset inventory. Only with that, possibly dangerous network or host activity can be detected. Such detection is usually offered by IDS that lookout, e.g. on network tabs or SPAN ports, for anomalies in the network traffic. Compared to traditional IT networks, this is a quite promising approach, since—in contrast to IT networks—the expected network traffic does not vary much such that false positives can be relatively easy tuned to a minimum. A more active approach to IDS is threat hunting. [...]
When it comes to suitable mitigation strategies, the first line of defense to strengthen are the humans operating ICS. As stated in Subsection 3.3, many adversaries use social engineering for gaining an initial foothold in the victim's network. The risk of successful phishing compromises can e.g. be reduced by security awareness workshops. More on the technical side of things are vulnerability management solutions. In ICS environments, it is often not that easy to patch hosts, since this could mean downtime and therefore revenue loss. However, it is crucial to at least know which hosts have known vulnerabilities. Even if a patch might not be possible, one could e.g. at least harden the network segmentation around the vulnerable hosts to make a compromise less likely. Inspired by traditional IT networks, firewalls are becoming more and more popular in ICS environments, too. They are especially critical in overlapping parts of the IT and ICS networks. Last but not least, it is essential to have a solid backup strategy which allows for restoring operations fast and reliable, e.g. in the case of a ransom- or wiperware attack.

4 Detailed Analysis of the Triton Attack

While the previous section conducted a comparative overview of the most prevalent ICS security incidents to highlight general trends, this section focusses on a single attack to detail how insight gained from such an analysis can be used to prepare for future attacks. Exemplary, the Triton attack targetting a Saudi Arabian petrochemical plant in 2017 is analyzed. The incident—also known as Trisis [12] and HatMan[4]—is chosen as an example for several reasons. First and foremost it was the first attack targetting SIS and therefore potentially threatening human lives. Additionally, the attack was highly sophisticated and even when it was eventually detected by the plant operators, they were not able to stop it immediately. For these reasons, Triton is considered to be of significant importance to the ICS community [12].

[4] https://www.us-cert.gov/ics/MAR-17-352-01-HatManSafety-System-Targeted-Malware

4.1 Attack and Response Strategies

As described in Subsection 3.3, an ICS attack usually is comprised of the two stages of the ICS Cyber Kill Chain. When it comes to Triton, the details of stage one are still unclear. It is not unambigously known, how the IT network of the Petro Rabigh oil refinery got breached in the first place and how the attackers moved from there into the ICS network. It is suspected, however, that the initial access happened via a spearphishing attack. [citation]
Stage two of the ICS Cyber Kill Chain is mainly performed by a malware focussed on ICS effects which is nowadays known as Triton. The attackers managed to install this malware on the Triconex SIS from Schneider Electric—therefore the name Triton or Trisis. SIS are an integral part of ICS in that their sole purpose is to maintain safe operations should failures of other hard- or software occur. They should prevent catastrophic incidents like explosions or fire [6]. It is therefore crucial that this last line of automated safety denfense operates correctly. The functionality of a SIS can be broken down as follows. The inputs for a SIS are an array of sensors measuring physical values e.g. temparature, pressure or rotation speed. In real time, the SIS analyzes these values and outputs a single decision: if it is safe to continue operation. Should the SIS decide that there is an unsafe physical condition, suitable commands are sent to according actuators like water pumps, machine engines or valves. E.g. if a SIS would detect a dangerously high temparature in a gas tank, the valves regulating the gas inflow would be closed. [12]
To protect a SIS from unintended modification, there is a physical keyswitch indication the mode of operation. Under normal circumstances this switch should be set to *run* which disables arbitrary changes to the logic of the SIS. In the case of Petro Rabigh, however, the switch was set to *program mode* which allows for logic changes. Why this was the case is not known, but it might very likely be the case that an engineer programming the SIS simply forgot to switch it back to *run* mode. In addition to these modes of operation,network connectivity to a SIS should in theory be extremely limited if existant at all. In practice, for example, plant operators sometimes want to retrieve data from SIS in order to analyze them which is why they allow for more network connectivity than needed for reasons of convenience. This was also the case at Petro Rabigh (?) [citation]. [12]
Once the Triton malware was installed on the SIS it tried changing its internal logic.

4.2 Goals, Impacts, and Attribution

As of today, the motivations behind the Triton attack remain unclear. At least, there is no reason to believe that it was meant to be part of an espionage operation because no spyware tools like key loggers were used. Since the adversaries specifically targeted the SIS, it is more likely that the goal of the attacks was to cause disruption. One way to achieve this is to provoke a shutdown of the plant, which also happens to be the actual impact of the attack. In total, the oil refinery

was out of operation for multiple weeks. While this also implied monetary losses for the companies running the petrochemical plant, financial gain or harm does not seem to be the driving force behind the attack [8]. Another way of creating disruption is to cause an unsafe physical state leading to physical damage. [12] Potentially this could also lead to threats against human lives. Whether or not the latter was indeed part of the adversaries goals is still unknown.
The reasoning about the underlying motivations together with the fact that the attack required a tremendous amount of resources suggests that the threat actor behind the attack is a nation-state [8]. Indeed, the attackers behind the Triton operation seem to be a Russian threat group, given the name TEMP.Veles, which is probably backed by a Russian research institute based in Moscow [9], [3].

4.3 Detection and Mitigation Opportunities

5 Conclusion

References

1. Andy Greenberg: Crash override: The malware that took down a power grid. https://www.wired.com/story/crash-override-malware/ (2017), [Online; accessed 03-May-2020]
2. Assante, M.J., Lee, R.M.: The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room **1** (2015)
3. Blake Sobczak: The inside story of the world's most dangerous malware. https://www.eenews.net/stories/1060123327 (2019), [Online; accessed 09-May-2020]
4. Case, D.U.: Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC) **388** (2016)
5. CyberX: 2020 global iot/ics risk report (2020)
6. 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)
7. Dragos: 2019 - year in review: The ics landcape and threat activity groups (2020)
8. Eduard Kovacs: New 'triton' ics malware used in critical infrastructure attack. https://www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack (2017), [Online; accessed 09-May-2020]
9. FireEye Intelligence: Triton attribution: Russian government-owned lab most likely built custom intrusion tools for triton attackers. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html (2018), [Online; accessed 09-May-2020]
10. 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)
11. Huang, K., Siegel, M., Madnick, S.: Systematically understanding the cyber attack business: A survey. ACM Computing Surveys (CSUR) **51**(4), 1–36 (2018)
12. Inc., D.: Trisis malware: Analysis of safety system targeted malware. Tech. rep., Dragos Inc. (2017)
13. 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]
14. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ics) security. NIST special publication **800**(82), 16–16 (2011)
15. ThaiCERT: Threat groups cardss: A threat actor encyclopedia (2019)
16. 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)

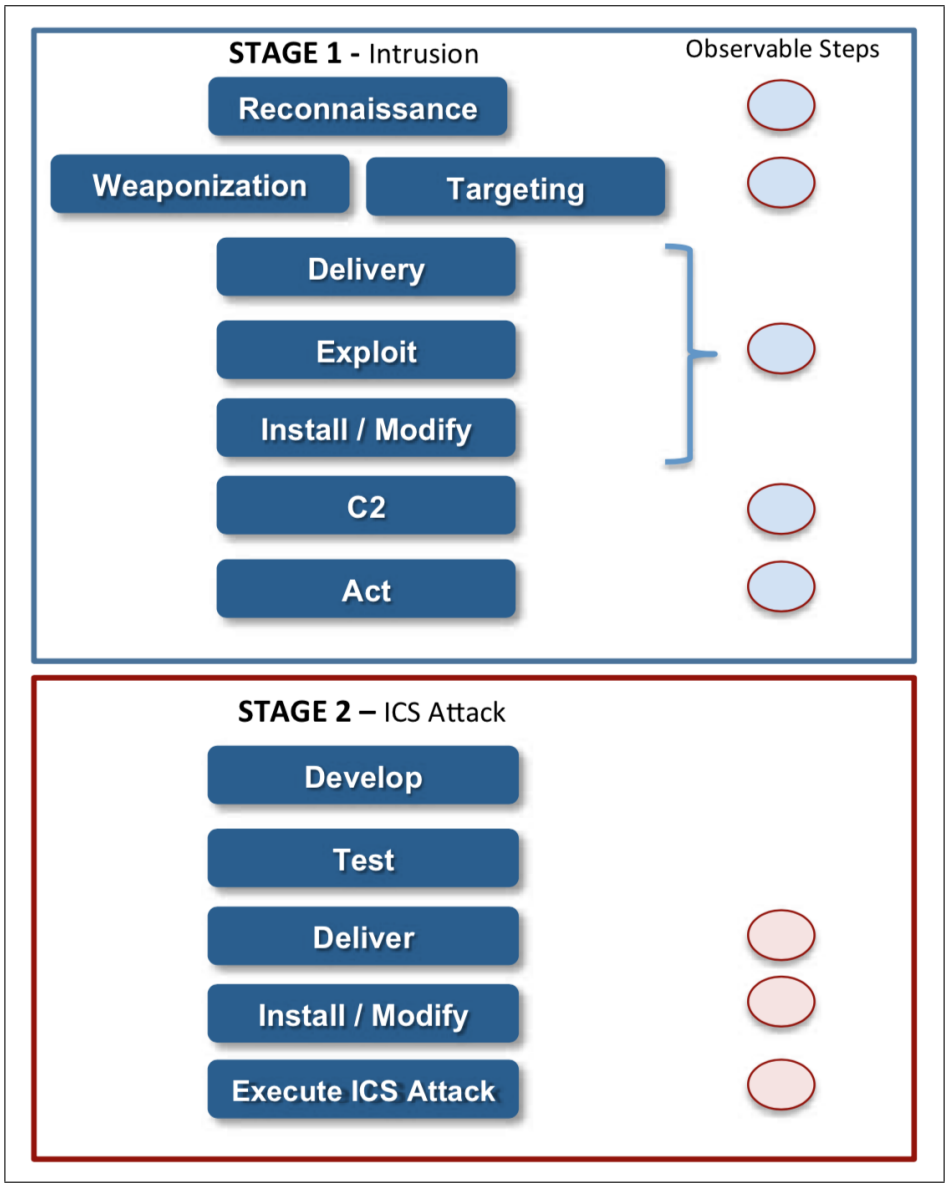

Fig. 1. ICS Cyber Kill Chain as introduced by the SANS institute, from [2].