2017

Cyber Security Incidents on Critical Infrastructure and Industrial Networks

Robert Ighodaro Ogie
University of Wollongong, rogie@uow.edu.au

Publication Details

Ogie, R. I. (2017). Cyber Security Incidents on Critical Infrastructure and Industrial Networks. ICCAE '17: Proceedings of the 9th International Conference on Computer and Automation Engineering (pp. 254-258). New York, United States: ACM.

Cyber Security Incidents on Critical Infrastructure and Industrial Networks

Abstract

National critical infrastructure and industrial processes are heavily reliant on automation, monitoring and control technologies, including the widely used Supervisory Control and Data Acquisition (SCADA) systems. The growing interconnection of these systems with corporate networks exposes them to cyber attacks, with several security incidents reported over the last few decades. This study provides a classification scheme for categorising security incidents related to critical infrastructure and industrial control systems. The classification scheme is applied to analyse 242 security incidents on critical infrastructure and industrial control networks, which were reported between 1982 and 2014. The results show interesting patterns, with key points highlighted for the purpose of improving the way we plan for and direct efforts toward protecting critical infrastructure and industrial networks.

Keywords

incidents, security, industrial, networks, infrastructure, cyber, critical

Disciplines

Engineering | Physical Sciences and Mathematics

Publication Details

Ogie, R. I. (2017). Cyber Security Incidents on Critical Infrastructure and Industrial Networks. ICCAE '17: Proceedings of the 9th International Conference on Computer and Automation Engineering (pp. 254-258). New York, United States: ACM.

Cyber Security Incidents on Critical Infrastructure and Industrial Networks

R.I. Ogie
Smart Infrastructure Facility,
University of Wollongong,
Wollongong, Australia
+61 2 4239 2535
robert_ogie@uow.edu.au

ABSTRACT

National critical infrastructure and industrial processes are heavily reliant on automation, monitoring and control technologies, including the widely used Supervisory Control and Data Acquisition (SCADA) systems. The growing interconnection of these systems with corporate networks exposes them to cyber attacks, with several security incidents reported over the last few decades. This study provides a classification scheme for categorising security incidents related to critical infrastructure and industrial control systems. The classification scheme is applied to analyse 242 security incidents on critical infrastructure and industrial control networks, which were reported between 1982 and 2014. The results show interesting patterns, with key points highlighted for the purpose of improving the way we plan for and direct efforts toward protecting critical infrastructure and industrial networks.

CCS Concepts

• Information systems applications → Process control systems • Security in hardware → Hardware security implementation.

Keywords

SCADA; Critical infrastructure; Industrial control systems; Cyber security; Cyber attacks.

1. INTRODUCTION

Modern industrialised societies are fast becoming heavily dependent on automation and control. On the one hand, the large and complex network of highly interconnected infrastructure assets such as electricity grids, water distribution systems and transportation facilities must be adequately monitored and controlled in order to optimally serve their intended purpose of enabling the flow of goods and essential services within urban and regional settings [1]. On the other hand, the industrial processes that generate economic prosperity for the society must be supported with automation and control technologies in order to safely attain optimal desired outcomes [2]. Supervisory Control and Data Acquisition (SCADA) systems provide the needed monitoring and control capabilities for real-time operations of these critical infrastructures and industrial control networks [3].

Historically, SCADA systems have been designed to operate in standalone networks, completely insulated from the corporate network [3]. However, with growing competition and increased pressure to reduce cost and improve operational efficiency, the need to share information with corporate business units as well as perform maintenance routines remotely has resulted in widespread interconnections of SCADA systems with corporate networks that are remotely accessible through the internet [4]. This growing practice, in combination with progress in using standard networking protocols for SCADA communications, has resulted in increased exposure of national critical infrastructure and industrial control systems to cyber attacks [5]. Consequently, there have been several reports of security incidents on critical infrastructure and industrial control systems, many of which lead to significant loss from economic, public safety and environmental standpoints [3].

Understanding the various dimensions of these security incidents and how they have evolved over time can indubitably provide insight for developing effective strategies to prevent or mitigate similar attacks in the future [5]. On this basis, Miller and Rowe [5] attempted to sample and classify past records of cyber attacks on critical infrastructure and industrial control systems. They classified attacks based on source sectors, method of operation, impact, and target sectors [5]. While their study contributes significantly in helping to understand the nature of previous cyber attacks on SCADA systems, the range of options considered in their classification scheme and the limited number of incidents (15) surveyed limits the ability to gain deeper insight into trends and patterns related to previous security incidents [5].

In the current study, an attempt is made to address this gap by presenting a more comprehensive analysis of previous security incidents on critical infrastructure and industrial control systems, both in terms of the range of options considered in classifying attacks and the number of incidents sampled. A total of 242 reported security incidents on critical infrastructure and industrial control systems are surveyed and analysed based on a proposed classification scheme presented in the following methodology section.

2. METHODOLOGY

This study was carried out using publicly available data from the Repository of Industrial Security Incidents (RISI) online database [6]. The data set covers industrial security incidents reported to have affected process control, industrial automation or SCADA systems within the period of 1982 to 2014 [6]. The data set remains one of the richest so far for understanding historical accounts of cyber attacks on critical infrastructure and industrial control systems worldwide. At the time of this report, the database contains 242 security incidents related to critical infrastructure and industrial control systems, most of which are confirmed to be correct. Attributes of the data include title, year, industry type, country/region, and a brief description of the incident, including its impact. The entire data set was analysed in order to show patterns and highlight key points that can be useful for how we plan and direct efforts toward protecting critical infrastructure and industrial control systems (ICS).

To ensure a structured analysis, incidents were classified according to the “intent”, “method of operation” and “perpetrator” of the attack.

2.1 Intent

This is the purpose for the attack as gleaned from the incident report. Based on the description of incidents, intent was classified into 7 categories namely theft, service disruption, unintended service disruption, sabotage, espionage, accident, and unknown.

Theft: This is theft of computers and other sensitive information such as intellectual property, trade secrets and other financial assets.

Service disruption: This refers to attacks wherein the intent of the attacker is to cause disruption, including delay and shutdown of services. The motivation to cause service disruption varies and can sometimes be due to the desire to expose the degree of vulnerabilities in industrial control systems. Based on incidents reported, service disruption could last from a couple of hours to few weeks.

Unintended service disruption: This covers incidents that results in accidental disruption to services. Based on incidents reported, unintended service disruption could also last from a couple of hours to few weeks.

Sabotage: This refers to attacks wherein the intent of the attacker is to deliberately cause damage to industrial control facilities or critical infrastructure networks.

Espionage: This refers to attacks wherein the attacker, often state sponsored, sets out to spy and collect information for political and military advantages.

Accident: This refers to attacks wherein the intent of the attacker is to cause accidents within industrial or critical infrastructure networks.

Unknown: This covers all other attacks in which the purpose was unknown.

2.2 Method of operation

Based on the classification of cyber attacks adopted in previous studies [7], [8], each reported incident was categorised into one of six methods of operation, namely malware, unathorised insider access, unathorised remote access, interruption of services, non-cyber attack, and unknown.

Malware: These are cyber-attacks that are carried out using malicious software. In order to infect the targeted network with malware, attackers often rely on the use of common techniques such as social engineering, phishing, and compromised removable media and personal laptops belonging to employees and vendors.

Unathorised insider access: This is when an insider (e.g. employee, vendor or contractor) gains access to computer resources in the corporate or industrial control network without the required permission. This type of attack can be carried out through different means including stolen credential, misuse of privilege, brute-force, and backdoor exploits.

Unathorised remote access: This is when an attacker remotely gains access to computer resources in the corporate or industrial control network without the required permission. This type of attack can also be carried out through stolen credential, brute-force, social engineering, and backdoor exploits.

Interruption of services: These types of attacks are aimed at interrupting or possibly shutting down essential services provided by industrial control systems and critical infrastructure networks. An example is denial-of-service attack, where the attacker aims to make the network unavailable [9]. Another example is *jamming*, where the radio frequencies that networked computers use for their wireless communication are interfered with [9].

Non-cyber attack: In industrial control systems, component failure (e.g. programmable logic controller), software bugs and computer malfunction or glitches can potentially result in the shutdown of crucial services. Incidents of this type are referred to as non-cyber attacks in this study.

Unknown: This covers all other attacks in which the mode of operation is unknown.

2.3 Perpetrator

Perpetrator refers to the alleged attacker responsible for the reported incident. In this study, perpetrators are categorised into lone hacker, organised hacking group, vendor, employee, unknown, and none.

Lone hacker: This includes any unaffiliated individual engaging in the cyber attack of critical infrastructure and industrial control systems on their own accord. Script kiddies, criminals and protesting members of the society often fall into this group.

Organised hacking group: These are highly motivated and well funded hacking groups. Examples include terrorist groups, hostile governments,

Vendor: This includes security vendors, suppliers and contractors.

Employee: This refers to disgruntled or greedy employees who attack their own employer’s system.

Unknown: This covers all other attacks in which the perpetrator is unknown.

None: This covers non-cyber attacks presented above, i.e., situations in which no one has deliberately launched a cyber attack on critical infrastructure and industrial control systems.

3. RESULTS AND DISCUSSIONS

The results of the analysis are presented and discussed in this section. Table 1 shows the number of incidents reported for each country. Europe appears in the list because of two reports of attacks on European facilities in 2003. About 17 countries recorded just one reported security incident. Others recorded more, with the United States topping the list followed by the United Kingdom. One may quickly interpret these results to be that the United States and the United Kingdom are the most vulnerable to cyber attacks on critical infrastructure and industrial control systems. However, given that the quality and completeness of records in the RISI repository are subject to people’s willingness to report security incidents, it could well be that the reason for the high level of incidents in the United States and the United Kingdom is because institutions are more open to share security incidents in these two countries or that the RISI data collection campaign is stronger in these countries.

Table 1. Number of reported incidents per country/region

Country or region	**Reported incident**
Brazil, Chad, Germany, Guam, Guyana, Italy, Lithuania, Norway, Poland, Qatar, Saudi Arabia, Spain, Sweden, The Philippines, Turkey, Venezuela	1
France, India, Ireland, Israel, New Zealand, South Africa, Europe	2
Iran, Russia	3
Switzerland	4
Japan	5
Australia	12
Canada	14
Unknown	16
United Kingdom	32
United States	123

Figure 1 shows the number of reported incidents for different critical infrastructure networks and industry types. Transportation topped the list (48), followed by Power and Utilities (45), Petroleum (36) and Water/Waste Water (31) in that order. Mining (1) and Pharmaceutical (2) were the least impacted by security incidents. One reason for the high level of attacks on transportation systems could be because of the many avenues to perpetrate such attacks- from road network (e.g. road signs attacks) to rail and air traffic systems; the reliance on automation and control systems creates many avenues for cyber attacks. Secondly, the wide geographical distribution and the huge impact associated with their failures make them attractive to cyber attackers. Same is true for the Power and Utilities sector. It should be noted that based on reports in the data set, the industry type, "Other" is observed to include facilities such as roller coasters, amusement park rides, hospitals, emergency services, military, etc.

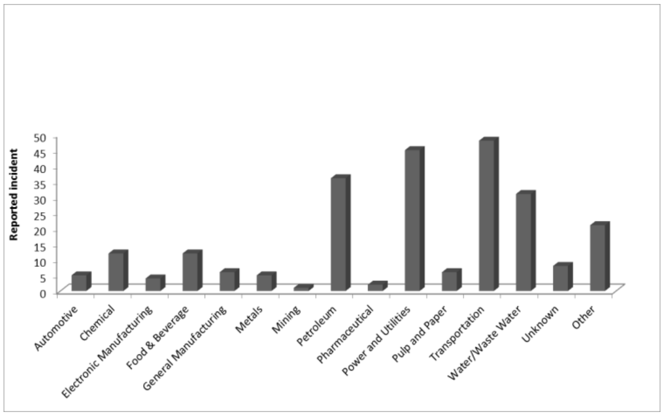

Figure 1. Number of reported incidents per industry type

The number of incidents reported for each year covered in the data set is shown in Figure 2. The highest number of security incident was recorded in 2003 (36), followed by 2009 (23), 2004 (22), and 2012 (19) in that order. A closer observation of reports within the data set shows rise in malware attacks from 2000, which peaked in 2003. After 2003, reported incidents dropped steadily until 2008. The reason for the drop cannot be gleaned from the data set.

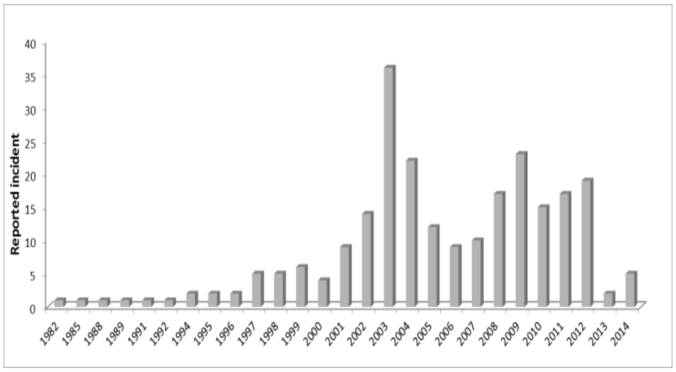

Figure 2. Number of incidents per year

3.1 Key observations from the results

- The first reported security incident on industrial control systems was in 1982, in which a Siberian gas pipeline exploded as a result of a Trojan that doubled its usual pressure. Though some sources claim that the explosion is due to poor construction and not malware, this incident is still recognised in the literature as the first reported cyber security attack on industrial control systems [5].
- More than half of all cyber attacks on critical infrastructure and industrial control systems (Figure 3) are aimed at causing service disruption. Attackers may adopt different methods of operation such as malware (e.g. worms, Trojans, viruses), unathorised access, and denial-of-service attacks in order to cause service disruption. Jamming (e.g. infrared and electromagnetic interference) also featured as a source of service disruption to critical infrastructure systems. Two reported cases of service disruption within the data set, i.e., the 14-year old school boy who hacked into Poland's tram system in 2008 and the 1999 Shut down of SCADA Systems in San Diego's water and energy facilities, involved the use of infrared remote control and electro mangnetic interference from a NAVY AN/SPS 49 radar operating off the coast of San Diego respectively.
- An Attack on a given infrastructure or industrial control facility may originate from multiple sources, making the tasks of mitigation and attribution difficult. A recent example reported within the data set is the 2014 German Steel Mill cyber attack, wherein multiple attackers succeeded in causing massive damage by putting a furnace in an undefined condition, so that it could not be shut down in the regular fashion.
- Many attacks on critical infrastructure and industrial control systems start by first gaining access to the corporate network before progressing to the control system network. This implies that while ICS and SCADA-specific security measures are crucial for the protection of critical infrastructure and industrial control systems, traditional approaches such as firewall, demilitarized zones, antivirus, intrusion detection and prevention, access control and authentication mechanisms must be put in place as the first set of security layers.
- Unauthorised access can occur remotely or through an insider. The results (Figure 4) have shown that insiders pose a similar risk of unauthorised access (8.26%) as do remote cyber attackers (8.68%). Adequate security policies and control must therefore be put in place to prevent insiders such as employees, vendors and contractors from gaining unauthorised access to computer resources.
- Figure 5 shows that approximately 66% of security incidents on critical infrastructure and industrial control systems are caused by unknown perpetrators while 17% are not caused by a perpetrator. Security incidents that are not caused by a perpetrator are likely to be non-cyber attacks. Non-cyber attacks constitute approximately 33% of security incidents on critical infrastructure and industrial control systems. Typical examples of factors observed to have resulted in non-cyber attacks on critical infrastructure and industrial control systems include lightning strike, inappropriate security practices (e.g. installation of incompatible antivirus and software patches in SCADA systems, unintended consequences from penetration testing and IT audits, etc.), incorrect network configuration, and poor management practices (e.g. incorrect network configuration, poor maintenance and upgrade of aged software and hardware

components resulting in system failure, inadequate staff training, incorrect programming of PLC controllers, etc.). These factors, amongst others, are also some of the reasons for the high record of unintended service disruption (18%) as shown in Fig 3.

- Approximately 5% of security incidents on critical infrastructure and industrial control systems are established to be caused by organised hacking groups (Figure 5). Some well-known hacking groups allegedly named as responsible for some of the reported cyber attacks includes the Anti Christ Doom Squad, Comment Group, Cutting Sword of Justice, Dragonfly, and Sun Hacker.
- Figure 4 shows that the method of operation for approximately 20% of security incidents on critical infrastructure and industrial control systems are unknown. This is a significant issue because the ability to protect systems from cyber attacks is degraded without adequate knowledge of the adversaries and their methods of operation.
- Common vulnerabilities exploited in many of the incidents reported includes uninstalled or outdated antivirus, inadequate firewall protection, lax physical security, use of weak or default passwords, inadequate security policies, poorly management backdoors, loopholes in ICS and SCADA products, employees as weak links in the security chain (e.g. the use of social engineering as well as the introduction of malware into the corporate network though connected personal laptops and USB sticks), poorly secured VPN access and other known vulnerabilities that are often associated with web services and windows systems.
- Some of the malware that have been successfully used against critical infrastructure and industrial control systems include Shamoon virus, Mariposa virus, Conficker virus, Stuxnet, PE_SALITY virus, W32.Virut.CF virus, Mytob worm, Ahack worm, Generic Backdoor.k Trojan, Zotob/PnP Worms, Spybot, W32/Korgo Worm, Sasser worm (rampant in 2004), Nachi/Welchia Worm, MUMU worm, Blaster virus (rampant in 2003), Nacchi virus, SQLslammer Worm, Sobig Virus, Nimda virus, Code Red Worm and the Remote Explorer. These malware, in addition to other SCADA-specific malware such as Flame and Duqu should be monitored as potential threats against critical infrastructure and industrial control systems [5].
- A total of 673 deaths were recorded while the number of injuries was well over 419. Most of the deadly incidents reported occurred in the transportation sector. One of such incidents is the 1997 Korean air line B747 CFIT accident that took 228 lives as a result of a bug introduced into the Minimum Safe Altitude Warning (MSAW) system during a software upgrade. Another 228 passengers also died in the Air France flight 447 that crashed into the Atlantic Ocean in 2009 due to suspected computer failure. The Spanair flight 5022 that crashed just after takeoff in 2008, killing 154 people is believed to be caused by a Trojan. In Australia, a Qantas Airbus A330 flight that plunged suddenly after experiencing a computer glitch in 2008 resulted in the injury of 110 people.

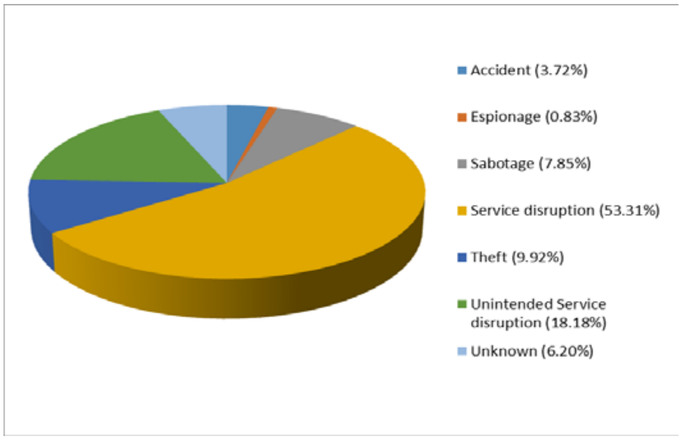

Figure 3. Distribution of security incidents by intent of attack

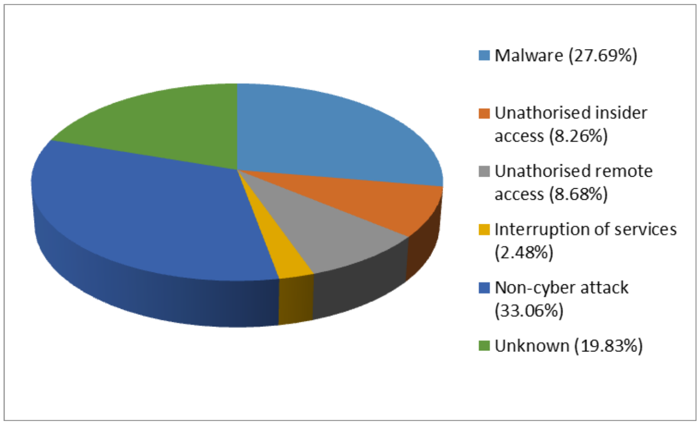

Figure 4. Distribution of security incidents by method of operation

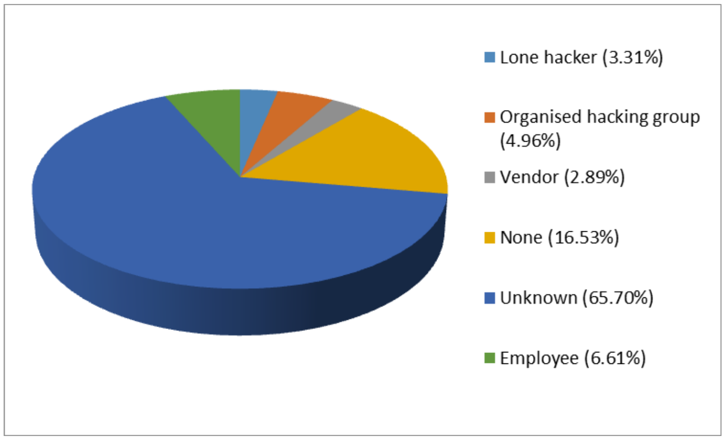

Figure 5. Distribution of security incidents by type of perpetrator

4. CONCLUSION

Cyber attacks on national critical infrastructure and industrial networks pose serious concern to modern societies. Understanding the evolution and the various dimensions of previous security incidents can help in developing effective strategies to prevent or mitigate similar attacks in the future. This study has presented a classification scheme for categorising security incidents related to critical infrastructure and industrial control systems. The usefulness of the classification scheme was demonstrated in analysing 242 security incidents on critical infrastructure and industrial control networks, all of which were reported between 1982 and 2014. The results revealed interesting patterns, including the most affected countries, the most vulnerable industry, the most prevailing type of attack etc. Furthermore, key points were highlighted for the purpose of improving the way we plan for and direct efforts toward protecting critical infrastructure and industrial control systems. One limitation of this study is the fact that availability and access to a complete record of all security incidents on critical infrastructure and industrial control systems is difficult, particularly when the area of interest is the global domain. The study used the most comprehensive data available publicly, but acknowledges that the incidents included in the data set are not exhaustive, even within the period investigated. Security incidents that occurred after 2014 are also not covered. Future studies will therefore seek to address these issues, including means by which governments, industry, private sector, academia and citizens can better work together to realise the shared responsibility of securing critical infrastructure systems through improved availability and access to comprehensive and accurate records of security incidents on SCADA networks.

5. REFERENCES

[1] Rice, J.A., Mechitov, K., Sim, S.H., Nagayama, T., Jang, S., Kim, R., Spencer Jr, B.F., Agha, G. and Fujino, Y., 2010. Flexible smart sensor framework for autonomous structural health monitoring. *Smart structures and Systems*, *6*(5-6), pp.423-438.

[2] Metzger, M. and Polakow, G., 2011. A survey on applications of agent technology in industrial process control. *IEEE Transactions on Industrial Informatics*, *7*(4), pp.570-581.

[3] Igure, V.M., Laughter, S.A. and Williams, R.D., 2006. Security issues in SCADA networks. *Computers & Security*, *25*(7), pp.498-506.

[4] Christiansson, H. and Luiijf, E., 2007, March. Creating a european scada security testbed. In *International Conference on Critical Infrastructure Protection* (pp. 237-247). Springer US.

[5] Miller, B. and Rowe, D., 2012, October. A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51-56). ACM.

[6] The Repository of Industrial Security Incidents, 2016. Accessed online on December 20, 2016. http://www.risidata.com/

[7] Ahmed, A.A. and Zaman, N.A.K., 2017. Attack Intention Recognition: A Review. *International Journal of Network Security*, *19*(2), pp.244-250.

[8] Ahmed, A.A., Jantan, A. and Wan, T.C., 2013. Real-time detection of intrusive traffic in QoS network domains. *IEEE Security & Privacy*, *11*(6), pp.45-53.

[9] Wood, A.D. and Stankovic, J.A., 2002. Denial of service in sensor networks. *computer*, *35*(10), pp.54-62.