Critical Systems Security: Analysis of Cyber Security Incidents in Critical Infrastructure

By Jacob John Williams

University of the West of England

15008632

1.0 Abstract

This paper reviews various threats to Critical Infrastructure from the last ten years, identifying their effect and operations within each sector. It then explores Critical Systems security methodologies, topologies, and devices. The final section of the paper is a brief look at newer standards and devices.

2.0 Introduction

Critical Infrastructure has existed for a long time, and the industrial control systems as we know them have existed from the mid-20th century. It was only up until recently that the key problem with industrial control systems was centred around operational hazards and the over all speed of the systems, but with the progression of technology bought more sophisticated ways to go about implementing such systems and automating parts of the process. This however bought many perils with it, some of which were unforeseeable. This paper will look at the threats that are directed at industrial control systems, as well as technologies and topologies to prevent attacks both already established and up-and-coming.

3.0 Threat Landscape

There are numerous examples of past threats that have targeted critical infrastructure, some to a near disastrous degree. The landscape is fairly broad not only because there are many threats but also because the threats to critical structures tend to cross the multiple sectors of industrial systems, for example an insider threat may occur solely in the field sector but an infection may occur in the enterprise sector and spread via network to the control and field sectors. In this section we will explore the threats not only by the sector in which they are most likely to occur, but also the direct or indirect effects it will have on other sectors.

3.1 Enterprise Sector

This sector is the business front of the Industrial Control System, it is where the more office centric roles operate. Rather than working directly with the industrial systems, this sector handles operations directly related to said systems; this could be finance, legal, human resources, and so on. The enterprise sector is reminiscent of your typical office network structure, usually being banks of computers connected to each other via conventional network topologies. All of this means that the Enterprise Sectors are open to all the threats that typical networks would be, such as Malware, Denial of Service, and other such attacks.

A particularly deadly example of an attack that could occur in the enterprise sector is Ransomware, which is a type of malware that encrypts files on the affected system and prompts for a ransom payment, in recent years this has been in Bitcoin but in the past it has occurred in other forms. The Ransomware often includes a countdown timer prompting for the payment by a certain time or the encrypted files will be deleted. There is no guarantee that files will be decrypted after the payment is made. The reason this threat is particularly notable is its method of initial infection, phishing emails. These emails are considered a form of social engineering, playing on operational, financial, or empathetic factors in order to get the target to download the malicious file or follow the suspicious link.

A notable example of a particularly deadly Ransomware attack is the 2017 WannaCry outburst. WannaCry is a Ransomware Cryptoworm that propagates through networks via an exploit dubbed ‘EternalBlue’, which used older Windows systems Server Message Block (SMB) protocol. Once it propagated to a system, the worm installs a back-door

called 'DoublePulsar' which would grant high levels of access on the infected system, allowing it to operate as it wishes *(ENISA, 2017)*. In 2017 alone WannaCry grew to infect 230,000 systems around the world affecting many different businesses, including: Telefonica, UK National Health Service, Deutsche Bahn, Renault, and more *(ENISA 2017)*. Whilst Ransomware may not pose a direct threat to systems in the field sector, a particularly deadly attack could propagate to the control sector from the enterprise sector and vice versa if the systems involved are outdated or security features are lacking. Even so, an effective attack on the enterprise systems may be enough to cause sufficient damage indirectly. The estimated damages to the UK National Health Service *(Department of Health and Social Care, 2018)* was 92 million pounds, occurring from directly damaged systems and operational downtime. This is further compounded by possible damage to the NHS' reputation due to the fact that the attack affected *(House of Commons Committee of Public Accounts, 2018)* 80 of 236 NHS trusts, a further 603 NHS organisations including 595 GP practices, which led to the NHS cancelling 20,000 hospital appointments and operations, and caused the closing of 5 accident and emergency departments. This was caused by the NHS utilising outdated systems, and is a clear exemplar of the financial and reputational damage that can be incurred by sophisticated malware attacks.

The cyber-attack on the Ukrainian Power grid in 2015 shares some similarities with the WannaCry attacks, mostly in its method of entry into the systems. The attack was a highly sophisticated and coordinated effort to bring down multiple energy stations around Ukraine, the objective appearing to be to create chaos and panic. Like WannaCry the initial infection was done via Phishing Emails typically phishing emails are akin to a "brute force" method, but the kind used in this attack were tailored to particular targets. This is what is known as Spear Phishing, the targets are usually ones considered to be the "weakest link in the chain" and they are typically observed in some fashion in order to garner information to use that would increase the effectiveness of the tailored phishing email. Unlike typical Phishing, Spear Phishing can also be undertaken over a longer period of time, waiting until a trust is built to be manipulated. All this creates an extremely effective method of infection, a study by *Lin et al (2019)* with a sample of 158 people of various ages and backgrounds showed showed that of the sample 43.3% (68 people) would click links contained in such emails.

The Spear Phishing campaign in this attack would have workers in the Enterprise sector of the Ukrainian Power stations download malicious documents which served as the delivery method, when the documents were opened it would prompt the user to enable macros. Once this was enabled, it would install the BlackEnergy3 malware on the system, which was connected to a command and control IP address allowing for communication and data exfiltration to the attacker. After this initial infection, the malware would scrape for credentials, escalate its privileges, and proceed laterally though the network. The attackers were quick to move from the foothold in order to avoid detection. Using the stolen credentials and elevated privileges, the attacker was able to pivot into network segments where the SCADA workstations and servers existed, the Control Sector. From there it would carry out its attack that would lead to the power outage affecting 225,000 people and last several hours *(E-ISAC and SANS-ICS, 2016)*.

A third case study for threats to Critical Systems is Stuxnet, a malware that some would disagree with calling a malware. Often referred to as the worlds first cyber-weapon, Stuxnet was a combination of numerous vulnerability exploits, including four zero days. Stuxnet would propagate through the air gap between networks via the exploitation of the LNK vulnerability, when a USB was inserted into a computer already infected with Stuxnet, it would rewrite Windows shortcut files to check for and install Stuxnet on the next device plugged into. Given this, Stuxnet would often enter into networks via a willing or unwilling third party. Once in a network, Stuxnet would propagate in a number of ways: A WinCC exploit targeting hard-coded passwords; the Print Spooler Zero Day (MS10-061) which allowed it to copy itself over networks using a compromised DLL; the Windows Server Service Vulnerability (MS08-067) in which it connected over Server Message Block (SMB) and sends a malformed path string allowing arbitrary execution to copy itself onto un-patched machines. Once it had infected a machine, it would install a Remote Procedure Call (RPC) server and client, using this it would communicate with other infected machines over the network to coordinate updates. This meaning that if a newer version of Stuxnet was introduced into the network, it could very quickly propagate it new features without having to re-compromise the machines. Using these network propagation methods and the air-gap USB drive method it would eventually enter the control sector, where it would then begin its attack *(Falliere et al, 2011)*.

3.2 Control Sector

The control sector is where the control centre operations occur, it is connected to the enterprise sector usually via a wide area network (WAN), and further connected to the field sector by serial radio communication. This sector typically contains the engineer's workstations, the control servers, the Human Machine Interface (HMI), and the data historian. It is typically organised using typical network topologies.

The Ransomware threat detailed in the previous section can also occur in the control sector, and in a particularly deadly manner. It can occur here in similar ways to the enterprise sector, via propagation from said sector, through malicious emails, or a compromised USB containing the payload. There are many machines in the control sector that are absolutely vital to the overall operation of the control network. Ransomware could infect and encrypt data on: The Data historian, which would cause the loss of a considerable quantity of data should it be unable to be recovered; the HMI station, which would create a condition where engineers are no longer capable of observing the data from the field sector and therefore unable to make informed decisions; or even the control server, which would completely halt all communication between the control and field sector.

The Control Sector is where the attack stage of the Ukrainian Power grid attack played out. It began by learning how to interact with the three distinct Distributed Management Systems using the native control present in the system and operator screens, and developing malicious firmware for the serial-to-ethernet devices. During this attack stage, the adversary used native software to deliver themselves into the environment for direct interaction with the ICS components, they achieved this by using existing remote access administration tools on the operator workstations. In preparation for the final stage of the attack, the adversaries installed a modified version of KillDisk, which would allow them to erase the master boot record, effectively locking users out of systems, and erasing targeted logs. At the time of attack, the adversaries used the Human Machine Interface to open the breakers, shutting off the power. Simultaneously, the adversaries would upload the developed malicious firmware to the Serial-to-Ethernet gateways, this was to ensure that even if the workstations were recovered that they still would not be able to issue commands remotely. During this period, attackers would also perform a remote telephone denial-of-service attack to prevent communication between the companies and customers, the objective of this particular part of attack is subject to debate.

When Stuxnet enters the control sector it would propagate through the aforementioned means but also perform the first stage of its attack vector, it would infect project files belonging to Siemens WinCC/PCS 7 SCADA control software. It would then intercept communication between WinCC and the target PLC devices, doing this, Stuxnet is able to install itself onto target PLC devices in the same way that the usual Step 7 project might be deployed. Using the same communication exploit, it would mask itself from WinCC if the control software attempted to read an infected block of memory. Once installed on the PLC's and therefore in the field sector, it would perform its key objective *(Falliere et al, 2011)*.

3.3 Field Sector

This sector is where the Programmable Logic Controllers (PLC) and the Remote Terminal Units (RTU) interact and control various machinery. It is connected to the Control Sector alone via serial-based radio communication.

The Ransomware threats detailed in the previous sections will have little effect here, and programming them to affect PLC's or RTU's would be extremely difficult if not impossible. The only thing that Ransomware could affect in this sector is the remote access computer, the malware wouldn't be capable of propagating via the Radio connection from the control sector, so therefore the only method of propagation to the remote access computer would be via infected USB.

In the case of the Ukrainian Power grid attack, the Field Sector wasn't compromised, but the Control Sector machines that controlled them were. Theoretically, the only way the attack on the grid could directly compromise the field sector would be if a remote access machine local to the field sector was compromised, but given the method of propagation this is very unlikely.

Stuxnet has a completely different objective to the previous case studies in the Field Sector. For the most part the previous cases didn't directly affect the Field Sector, but rather denied access to it via its operations in the Control Sector. This is in part due to the devices in the Field Sector being limited in memory and therefore complex to attack, or simply because the attacks were not intended to attack them. Stuxnet is programmed to target particular SCADA configurations, meaning that unless the PLC is identified as its target it will remain dormant. In the original case of Stuxnet,

once it had attached to the Siemens S7-300 system and identified PLC systems from the Vacon or Fararo Paya vendors that run between 807 and 1210 Hz, it would frequently modify the frequency from 1410 to 2 to 1064 Hz. This would cause the physical destruction of the centrifuges controlled by the PLCs *(Falliere et al, 2011)*.

3.4 Methodologies and Technologies By Killchain Stages

The previous section detailed threat capabilities on a case study basis, for a broad overview of various technologies and methodologies used in a variety of attacks refer to *Appendix A*. All information is drawn from *Tarun and Yadav (2016).*

4.0 Security Approaches

Security in critical systems is primarily concerned with the intercommunication of devices and the networks at large, physical intrusion through either a willing or unwilling party is difficult to protect against due to its unpredictability, meaning the priority of network security in critical systems is to prevent mapping and subsequent propagation. NIST (2015) defines numerous methods of implementing security among ICS networks, where most of the content in this section will be garnered from. More recently the BSI (2019) have also defined a document detailing security standards, however this document is still in production and while there are numerous available drafts, using its contents in this paper may be difficult.

As seen in the threat landscapes section of this paper, most threats appear to begin their attack vector through the Enterprise sector, often introduced through a willing or unwilling third party, but it is then the applications and protocols within the Enterprise Sector that allow it to pivot into the Control Sector. Due to this one must make a substantial design choice, if the Enterprise and Control Sector are completely disconnected then it removes a lot of work and attack vectors. It is often the case however that separating the two entirely is out of the question, due to the cost of ICS installation and maintaining a homogeneous network infrastructure requiring a connection between the two (NIST, 2015). This connection does present a significant security risk, and should be monitored by Boundary Protection devices, which will be detailed later.

Before exploring devices used to create security, one must explore a concept broached in the previous paragraph, the separation of the networks contributes greatly towards the deployment of security devices. NIST (2015), defines this as *"Network Segmentation and Segregation"*, working to establish security domains managed by the same authority, enforcing the same policy, and having a uniform level of trust. Typically the segmentation and segregation is implemented at the gateways between domains. For the most part, this paper has already utilised the standard separation in its format, separating into the Enterprise, Control, and Field networks and implementing security between them. There are three different types of separation, viewable in Appendix B, but for the most part we will be looking at Network Traffic Filtering as a methodology and its technologies. Regardless of methodology or technology, there are four key concepts that implement *Defense-In-Depth* by providing good segmentation and segregation. Firstly, apply technologies at more than one layer to broaden security. Secondly, use the principles of least privilege and need-to-know in order to organise your structure. Thirdly, separate information and infrastructure based on security requirements. Fourthly and finally, implement white-listing rather than black-listing, you should be in control of who enters the network not attempting to determine who shouldn't be entering.

Boundary Protection is the concept of implementing security devices on the connections between the sectors in order to control what is passing amongst them. In essence, Boundary Protection Devices determine whether data transfer is permitted by examining the data or meta-data. The first kind of device is the most known, the Fire Wall. These devices restrict ICS inter-sub-network communications and prevent unauthorised access to the respective systems and resources within the more sensitive areas. There are three types of Fire Wall, the first is Packet Filtering which operates at the Network Layer (layer 3) and is a routing device that includes access control functionality for system addresses and communication sessions. Packet Filtering Fire Walls check the basic information in each packet, such as IP address, and can either drop, forward, or message the origin. The draw back of this type is the overhead created by checking process, which is considerable for a network that relies on its near instantaneous updates. The next type is Stateful Inspection, which operates at the Network (layer 3) and Transport (layer 4) layers, and it contains functions to evaluate the contents of the packets on both layers against rule sets in order to confirm legitimacy. The third type is Application Proxy Gateway, operating at the Application Layer (Layer 7), and it examines the packets being pass among the applications, filtering based on rulesets. It offers high level of security, but

also a considerable overhead. Fire Walls are known as Dual-Homed devices, meaning they exist in two different networks at once, and in ICS they should be the only Dual-Homed devices.

Another form of Boundary Protection is the Demilitarized Zone (DMZ), which is a host or network segment that acts as a neutral zone between security domains. Such zones are created to allow for greater control and monitoring of traffic between two sectors by enforcing the domains information security policy for information exchange. It also works to provide sectors with access to devices in other sectors while shielding the sectors from external threats. NIST (2015) defines a number of roles the DMZ can fill, but the key ones are

i. Implementing a white-list policy.

ii. Implementing Proxy servers as intermediaries.

iii. Preventing data exfiltration with packet inspection.

These two methods of boundary protection are the key to creating a secure ICS network. Combining these, along with routers and our method of network segregation we can look at how to position them. NIST (2015) recommends placing a router leading into a Fire Wall between the Enterprise Sector and the Control Sector. The router offering basic packet filtering capabilities and the Fire Wall performing more heavy duty content analysis to provide secure communications. Between the Control and Field sectors, NIST (2015) recommends a Fire Wall leading into a DMZ containing the Data Historian and the Data Server, which then leads into secondary Fire Wall. The contents of the DMZ are devices frequently accessed by both sectors, and therefore accessible by both through only a singular Fire Wall. The first Fire Wall blocks arbitrary packets, and the second Fire Wall can prevent unwanted traffic from a compromised server from entering the control network, and prevent control network traffic from impacting the shared server (NIST, 2015). The essence of deploying security in an ICS system is to make life as difficult as possible for would be attackers, which is why implementations often contain more than a singular Fire Wall. In short, the more changes to detect or at least delay the attacker, the better.

5.0 Improving Security

Critical Systems differs from no other area in Cyber Security when it comes to an exponential growth of innovation and devices, in this section we will broach some of the newer devices and methodologies being created or utilised.

Mentioned briefly in the previous section of this paper was the British Standards Institute implementation of the NIST (2015) standards in the European zone. These standards will be more up to date than the NIST ones, as by the time the standards are finalized and version one is published, it will be five years younger than the NIST standards. Furthermore, after reading through and comparing the two briefly, it would seem that thus far BSI (2019) is more detailed and explicit than NIST (2015).

A further technology being developed is Toshiba's CYTHEMIS, a device that is utilised to visualize control systems and industrial production systems in a single control platform. The CYTHEMIS boasts an End-to-End security solution to protect critical infrastructure control systems and industrial control systems that utilize IoT. The end-to-end solution includes numerous external hardware devices and softwares, allowing for security against authorized access and malware infections between its endpoints, all whilst being visualized, as well as preventing USB propagation. The CYTHEMIS hardware devices sit between the network and the varying devices, essentially monitoring and controlling the input and output of the device. Because of the network based characteristic, Toshiba boasts the ability to secure even older operating systems and equipments including legacy systems and discontinued platforms. This boast is hard to contest, given the physical nature of the device one would not have to update or patch the actual system itself, but merely the security device. What sort of overhead this device presents is unknown, as little documentation exists about it. One could also argue that the concept of supporting legacy systems with newer security measures is counter-productive, as it may encourage the use of older systems for cost effectiveness despite them being a danger to the network or even the workers around them.

6.0 Conclusion

Critical Systems have existed for a long time, and before the sharp rise of malware and the utilisation of computing on a world stage it had little to worry about in terms of network security, instead often focusing on the risks within; such as insider threats and corporate espionage. But this has changed, Control and Industrial systems have changed along with all other technologies and with it has it brought many dangers unrecognised until exploited. Before Stuxnet nobody thought about the possibility of utilising a malware as a precision weapon for targeting manufacturers, before the

Ukrainian Power Grid hack not many considered the impact a coordinated and sophisticated attack could have on vital systems. Its only due to these sort of events that security in these systems is beginning to catch up, however as with most systems in the field of Cyber Security, we should always assume the attacker is ahead of us. Fortunately in this case the attacker being far ahead gives us a clear objective, and that is to create innovative ways to secure these systems and put in place standard to guide organisations in defending against such threats. This is already beginning to happen, the BSI (2019) standard and Toshibas CYTHEMIS are merely examples, and future years will bring much more that will allow us to even the playing field in an area where the attacker is miles ahead.

7.0 References

British Standards Institute (2019) *EN IEC 62443-4-2 Security for Industrial Automation and Control Systems.* London: British Standards Institute.

British Standards Institute (2018) *EN IEC 62443-3-2 ED1 Security for Industrial Automation and Control Systems.* London: British Standards Institute.

Department of Health and Social Care (2018) *Securing Cyber Resilience in Health and Care: Progress update October 2018* [online]. London: Department of Health and Social Care. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf [Accessed 07 February 2020].

ENISA (2017) *WannaCry Ransomware Outburst*. Available from: https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst [Accessed 03 February 2020].

E-ISAC and SANS-ICS (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid*[online]. Washington DC: E-ISAC and SANS-ICS. Available from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Falliere, N.F., O'Murchu, L.O. and Chien, E.C. (2011) W32 Stuxnet Dossier. *Symantec Security Response* [online]., pp. 1-70. [Accessed 07 February 2020].

House of Commons Committee of Public Accounts (2018), *Cyber Attack on the NHS: Thirty Second Report of Session 2017-2019* [online]. London: House of Commons. Available from: https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf [Accessed 07 February 2020].

Lin, T.L., Capecci, D.E.C., Ellis, D.M.E., Rocha, H.A.R., Dommaraju, S.D., Oliveira, D.S.O. and Ebner, N.C.E. (2019) *Susceptibility to Spear-phishing Emails: Effects Of Internet User Demographics and Email Content*. Acm Transactions on Computer Human Interaction [online]. 26 (5) [Accessed 16 February 2020].

National Institute of Standards and Technologies (2015) *NIST.SP.800-82r2 Guide to Industrial Control Systems (ICS) Security.* Maryland USA: National Institute of Standards and Technologies. Available From: http://dx.doi.org/10.6028/NIST.SP.800-82r2 [Accessed 03 February 2020].

Toshiba (2019) *Control System & Industrial IoT Security Solution CYTHEMIS.* Available From: https://www.toshiba.co.jp/sis/en/scd/iotsecurity/index.htm [Accessed 03 March 2020].

Appendices

A. Broad Scope Threat Methodologies and Technologies

All data from *Tarun and Yadav (2016).*

Stage	*Methodology / Technology*	*Description*
Recon	*Target Identification and Selection*	*Passive* *Domain names, whois, records from APNIC, RIPE, ARIN*
	Target Social Profiling	*Passive* *Scraping social networks, public documents, reports and corporate websites.*
	Target System Profiling	*Active* *Pingsweeps, Fingerprinting, Port scanning*
	Target Validation	*Active* *Spam Messages, Phishing emails, social engineering*
Weaponization	*Remote Access Tool (RAT)*	*Executes on target system, giving remote, hidden, and undetected access to the attacker.*
Delivery	*Email Attachments*	*Content composed to entice the user by using appealing content.*
	Phishing Emails	*Sensitive information like Usernames, passwords, credit card details are extract masquerading as a trustworthy source.*
	Drive By Download	*Target is forced to download appealing malicious content from the internet. Images, PDF Word documents.*
	USB Removable Media	*Removable media devices which silently infect other systems by opening files.*
	DNS Cache Poisoning	*Divert internet traffic from legitimate servers to attacker controlled destinations.*
Exploitation *(Exploits are usually combined into a singular, multi-exploit kit)*	*Operating System Level*	*Kernal, device drivers, denial of services, remote or local code execution.*
	Network Level	*FTP, SMTP, NTP, SSH, router, privilege escalation.*
	Application Software	*Browsers, MS Office, PDF, Java / Flash, Memory Corruption (Dangling-pointer,buffer overflow, use-after-free)*
Installation	*Droppers*	*Program to install and run malware on system. Will try and disable device security.*
	Downloaders	*Similar to dropper, smaller, connects to a remote server and downloads the rest of the payload.*
	Anti-AntiVirus	*Dropper and Downloader are usually "armoured", containing toolsets for disabling security measures, changing DNS to prevent updates.*

	Rootkit and Bootkit	*Payload file hiding, process hiding.* *Bootkits hook and patch system to gain kernal access.*
	Targeted Delivery	*Preventive measures against deploying malware in a virtual environment.*
	Host-based Encrypted Data Exfiltration	*Critical data stolen is encrypted and sent over a clear text protocol such as HTTP or SMTP.*
Command and Control *(Architecture)*	*Centralized*	*Single Server, no dependency on peer-to-peer. Infected machine failure wont affect the whole. Take down of C&C will bring down entire structure.*
	Decentralized	*Peer-to-peer. Scalable. Fault Tolerant.*
	Social Networks Based	*High Availability. Reliable. Profiles used to pass on information.*
Command and Control *(Secure Communications)*	*IRC Chats*	*Application layer protocol. Client / server networking model.*
	TCP / HTTP	*Secure, error checked, over the web communication protocols.*
	Steganography	*Encoding information in images, video, or audio.*
	TOR	*Hidden service protocol. Traffic directed through a worldwide volunteer overlay network.*
Command and Control *(Obfuscation)*	*DNS Fast Flux*	*Rapidly changing network of machines*
	Domain Name Generation Algorithm	*Pseudo Random Domain Names.*
Act on Objectives	*Mass Attack*	*Distributed attack on many targets. General target is credentials. Bigger picture is botnet creation.*
	Target Attacks	*Generally more sophisticated. Carried out with caution. Aim is to acquire confidential data.* *Data Exfiltration and acquiring user credentials for online accounts are the objectives.* *Distributed propagation could be a goal.*

B. NIST Network Separation Methodologies and Technologies

NIST (2015)

Logical Network Separation	Enforced by encryption or network device-enforced partitioning.	Virtual Local Area Networks (VLANS) Encrypted Virtual Private Networks (VPNs) Unidirectional Gateways
Physical Network	Complete separation to prevent interconnectivity of traffic between domains.	N/A

Separation		
Network Traffic Filtering	Utilize a variety of technologies at various network layers to enforce security requirements and domains.	Network Layer Filtering State-based Filtering Port / Protocol Level Filtering Application Filtering