An overview of Physical Cybersecurity **4/21/2024**

BS:Cybersecurity

Justin Saldivar

Old Dominion University

ABSTRACT:

In the world of cybersecurity, the focus of most operations pertains to the defense of networks, computers, and servers. This is reasonable as these systems are often the foundations in which governments and organizations operate and thus are enticing targets to cripple if not outright control as the information and computing power these systems have can be utilized in a wide variety of ways, they are not the only consideration when it comes to cost and importance. Physical systems and locations, such as power plants, server buildings, and even basic heating and door controls can be at risk of attack, infiltration, or even outright control. The question is: what can be done to protect these locations and systems from hostile parties seeking to inflict damages for their own ends?

Key Words: Infiltration, Security, Defend

INTRODUCTION:

As time goes on and infrastructure becomes modernized. More systems in the real world such as door systems, pressure control in pipes, and even power systems are integrated with online networks or use a terminal to control. This allows for easy control and access of critical systems, known as Cyber Physical Systems (CPS). These systems are integrated into both the private sector and government affiliated facilities, most importantly, however. These systems can control major utilities responsible for public services such as power grids, water, and fuel lines, and even communications systems can all be controlled by someone on a terminal who may not even be in the same location as these critical systems. This can be incredibly dangerous for national security should these systems become compromised and hijacked by a third party for their own ends.

These attacks can range from the disabling of pipelines via a command to the control unit to halt the stream to the outright destruction of these systems without any physical tampering. such as the overloading of a power station via a simple command to the terminal attached to it. Most importantly however is the way these systems can become infiltrated, either the hack comes from another location, necessitating improved cybersecurity. Or worse, an inside agent infiltrates the physical location of these important utilities and bypasses both conventional and cyber defenses and sabotages from the inside with ease. Therefore, not only is it crucial that these foundational systems and the electronic components that can control them be defended by hostile third parties in cyberspace. An organization must ensure that the risk of physical infiltration and uploading of dangerous malware by an insider remains only a theoretical and not reality. To this end this paper will both explore how these vital systems can be put at risk both electronically and physically and detail the various defense methods and strategies used to ensure that these utilities remain secure for all to use without fear.

RISKS INHERENT:

To begin with this section, the identification of points of security failure for network and computer connected utilities and the security of physical locations will be documented, starting with network weaknesses. The first weakness that could be exploited are the devices themselves, outdated machines with no prospects of support are a prime target for a potential attack, as if a vulnerability is discovered. It can easily be exploited and kept secret as the manufacturer has long since abandoned maintenance and updates of the outdated machine. Next, should the machine operate the utilities wirelessly via radio waves and no form of checking is done for the integrity and validity of commands, a hostile party could use this wireless connection to hijack the machine from a foreign location. Giving them free reign over the machine effectively. Finally, should a data breach occur in a network controlled system, whether by accident or a purposeful leak and information is revealed to the public, the possibility of a third party using the data to either exploit it for monetary gain or use the data to coordinate an attack would prove disastrous to Cyber Physical Systems (Konstantinou, Maniatakos, Saqib, et all, 2015).

Just as important as network and computer defense is the physical defense of the locations containing these vital units with several potential dangers associated with this field, the first danger is from employee infiltration. Without good background checks and inspections alongside training, an intruder can bypass security quite easily without much resistance. This could be accomplished either through the impersonation of other job roles such as a janitor or inspector or even through an air of authority, employees may fail to realize the person they just opened the door for was a threat if they had the appearance of someone important or looked like they belonged. The next concern is unsecured entrances of several types, this does not just mean easy to access entrances and bypassable perimeter security. It also includes little to no internal security and open areas. This connects to the previous ideas of an infiltrator as without locked doors to critical locations such as a server room, an intruder could easily walk in and fulfill their objectives with little to no resistance.

Worse still, should a USB port, Ethernet port, or even a Wireless router be available for exploitation, an attacker could easily slip in an infected drive or upload their malware directly into the network either through a plugged in laptop or wirelessly. This can quickly take a toll on the network and the physical systems connected to it with security none the wiser until it is too late and the damage is already done (Konstantinou, Maniatakos, Saqib, et all, 2015). There is historical precedent towards this. In 2007, the first instances of what would eventually be known as Stuxnet were allegedly slipped into exposed USB ports on a water pump installed at Iran's nuclear enrichment centers by an inside agent. Which, once inside the system, used false certificates and a zero day vulnerability present in the digital controllers used in the refining process to speed up the centrifuges responsible for nuclear refinement to dangerous levels while also sending out false positive reports to misdirect engineers. Causing great damage over several years (Kushner, 2013, accessed 4/21/2024).

To quickly summarize this section, the risks can be divided into two parts. The network vulnerabilities which include zero-day and unsupported hardware or software, unverified wireless systems which can accept any command so long as they can directly communicate with the system, and finally unshielded network traffic being a prime target for easy listening and hijack operations. Then would be physical vulnerabilities with the first being poor vetting and

employee training allowing for easy infiltration, next would be unsecured entrances to key areas such as server rooms and even back doors, finally would be unprotected network access from exposed USB ports to unsecured network entrances such as open ethernet cables and easy to access wireless networks.

PHYSICAL ASSET PROTECTION:

With the risk vectors very clearly shown. It would be unfair to not show potential countermeasures that could be taken to ensure the security of the networks and devices in charge of vital utilities necessary for public use. To protect a network from the potential of attacks on zero-day vulnerabilities and unsupported machines. An effort should be made to regularly upgrade machines whenever possible to currently supported versions. However, Caution should be taken, as updating to an updated version of a machine or software could invite disaster as zero-day vulnerabilities have not likely been discovered yet. A system of cautious upgrading wherein crucial systems is on supported hardware and software with the ability to rollback should a vulnerability be discovered in a updated version or hardware could protect critical systems from the possibility of attacks from both ends of the age spectrum.

Next, to ensure that a wirelessly connected machine will only accept orders from affiliated devices. There are several ways to accomplish this, the first is to filter based off MAC (Media Access Control) addresses. Allowing only devices verified by the system to connect to other devices. Another way is to implement data encryption, this is to ensure that whatever order sent to a machine will be much harder to read by an outside third party. It is much less replicated if the connection between the proper client and machine are already being monitored for intrusion (dig8ital, accessed 2024).

Finally, although data leaks are unpredictable as they may happen at any time from a wide variety of sources and events, there are measures that can be taken to protect data from being revealed to the wider public. Strict password and logging policies alongside employee training on what to do in a potential leak can go a long way in reducing the chance of vital data being exfiltrated by third parties for their own ends (Fortinet, accessed 4/22/2024).

To summarize, a policy of consistent upgrades with rollback schemes can protect against outdated electronic based attacks and zero-day attacks, various monitoring and encryption schemes can protect wireless controls and access from third parties, and a stringent password and employee training can reduce the likelihood of a data breach.

PHYSICAL LOCATION PROTECTION:

In the same vein as the last point above, there are several methods in which to physically defend a vital location and its access to important utilities from a physical infiltration. To ensure that an intruder does not simply waltz in on false credentials and bravado.Individuals not a part of the staff lineup should not only be inspected for potential holes in their story of employment, but should also be constantly monitored to see if their claims of who they are remain true. Additionally, employees should also keep an eye out on individuals asking to get by or enter a room typically closed off to visitors. Unless explicitly informed that the individual is trustable. The visitor should only be kept in areas away from sensitive systems such as a server room or machinery with wireless connections. Should something be amiss about the visitor, security can be called to sort the situation out although they must take care to not interfere too greatly in the standard operations of the building the machines are situated at (Lee, 2020).

Of course some infiltrators choose a more indirect route to physical systems to do damage. To discourage this, various things can be done. From the installation of various fences and light posts to discourage approach psychologically, to actual guards patrolling to make access harder. Additionally, the use of timed keycards to open certain doors and held only by certain individuals can prevent further ingress into the building itself or the rooms themselves, which should always be locked when not in use and if they are needed. Such as for server or machine connected maintenance, this brings up the last point as well. Anything that can allow for connection to either a machine or the local network must be tightly controlled. Electronic devices hooked directly to the network such as PC's, IoT compatible machinery, and the Servers should be locked away into secure locations to prevent the potential injection of malware via drive. In this same vein, the ethernet port and router should too be secured to prevent direct access to the

local network, ethernet ports can be directly disabled to prevent unauthorized connections to the network via port configuration software (EtherWAN, accessed 4/22/2024). The routers themselves and their associated network should both be secured, with the router in a locked room that requires credentials or a key and the network protected with a strong password (Lee, 2020).

To summarize, to physically protect the machines responsible for critical utilities. There should not only be physical deterrents such as high walls and lights, there should also be a great emphasis put on internal security. From the protection of ports to the network to the physical defense of the machines from intrudes by keeping them in hard to reach places.

CONCLUSION:

As more critical infrastructure becomes entwined with the digital world, a greater risk of catastrophic damage to vital services such as power and water becomes reality. There are several ways this could happen, from the physical infiltration of the locations and uploading the malware from there to the interception of both offsite commands to these machines and the stealing of valuable data from the network to potentially allow for greater damage in the future. To ensure that this sort of damage is less likely to happen, a significant effort must be made to secure both the facilities that house these vital apparatuses and the network that connects them all. From physical security such as greater obstructions outside the building to a stronger employee training policy designed to prevent would-be infiltrators from easily getting what they want and reduce the likelihood of a leak occurring. Additionally, ensuring that both the network is well defended and the machines that run vital infrastructure remain up to date with new parts and software is a critical part of curtailing the potential damage that may occur. Although there is never a guaranteed way of protecting infrastructure vital for society to function, it is better that these policies and machines are updated sooner rather than later to prevent an attack that has no precedent for both the scope and the scale of damage left in its wake.

References

Wen, G., Yu, W., Yu, X. *et al.* Complex cyber-physical networks: From cybersecurity to security control. ("Networked Learning Predictive Control of Nonlinear Cyber-Physical ...") *J Syst Sci Complex* **30**, 46–67 (2017). https://doi.org/10.1007/s11424-017-6181-x

Lee J. Wells, Jaime A. Camelio, Christopher B. Williams, Jules White, ("Jules White: H-index & Awards - Academic Profile | Research.com")
Cyber-physical security challenges in manufacturing systems,
Manufacturing Letters,
Volume 2, Issue 2,
2014,

Pages 74-77,

C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic and Y. Jin, "Cyber-physical systems: A security perspective," *2015 20th IEEE European Test Symposium (ETS)*, Cluj-Napoca, Romania, 2015, pp. 1-8, doi: 10.1109/ETS.2015.7138763.

https://www.researchgate.net/profile/Aslinda_Hassan/publication/325575773_A_NEW_TAXONOMY_OF_INSIDER_THREATS_AN_INITIAL_STEP_IN_UNDERSTANDING_AUTHORIZED_ATTACK/links/60d94574a6fdccb745ecc689/A-NEW-TAXONOMY-OF-INSIDER-THREATS-AN-INITIAL-STEP-IN-UNDERSTANDING-AUTHORIZED-ATTACK.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail

https://www.proquest.com/openview/70523c95474a454446f743e8dab1a06d/1?pq-origsite=gscholar&cbl=55114

https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021_0.pdf
David Kushner https://spectrum.ieee.org/the-real-story-of-stuxnet
https://www.fortinet.com/resources/cyberglossary/data-breach
https://dig8ital.com/post/wireless-security-101/

https://www.etherwan.com/support/featured-articles/cybersecurity-tips-ethernet-networks#:~:text=Keep%20network%20equipment%20in%20restricted,rooms%2C%20or%20in%20lockable%20cabinets.&text=Disabling%20unused%20ports%20can%20stop,unauthorized%20access%20to%20the%20network.