PREVENTING A STUXNET LIKE ATTACK.

BY:

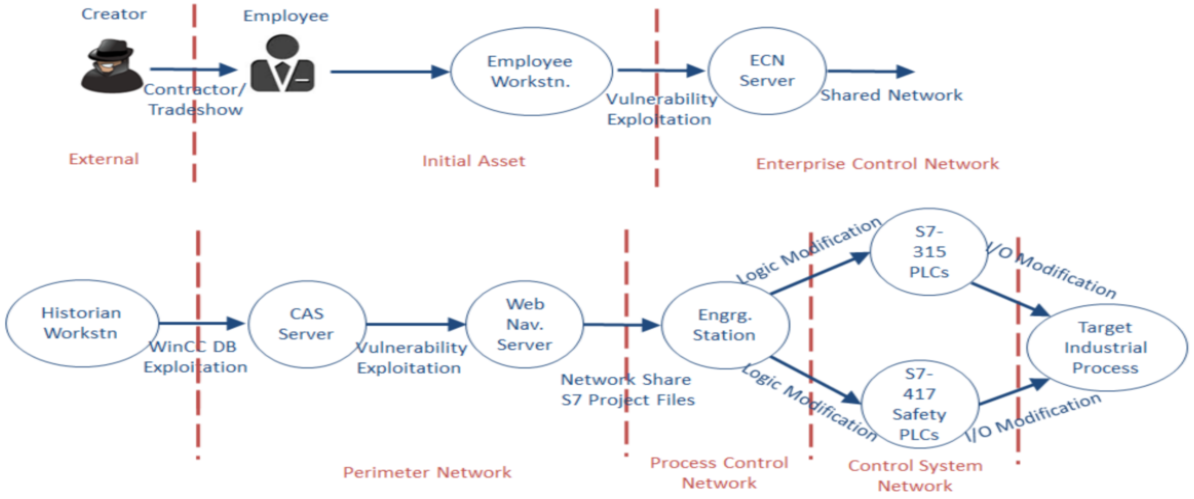
HARSHIT SHAKYA

(INDIAN INSTITUTE OF TECHNOLOGY, KANPUR)

ABSTRACT

In January 2009, officials from the International Atomic Energy Agency (IAEA) observed unusual circumstances at the uranium enrichment plant in Natanz, Iran. The centrifuges in Natanz were expected to remain working for about ten years, however due to the sensibility of the centrifuges Iran replaced up to ten percent each year. It was therefore relatively usual for Iran to replace around 800 centrifuges per year due to a variety of product defects and concerns regarding the maintenance. Officials from the IAEA believes that approximately 2,000 centrifuges were replaced by Iran between 2009-2010, and although the cause of the damaged centrifuges was right in front of them it took them almost a year to detect it. Later in 2010, a Belarusian computer security firm detected a new type of malware, later known as Stuxnet. Although the discovery of a new type of malware was neither unexpected nor uncommon, the character and sophistication of Stuxnet was certainly different.

Stuxnet is a cyber worm constructed to target a certain service on a very exact sort of Siemens software that are used in the crucial systems of Iran's nuclear facilities. The software systems that were targeted are in control of the frequency converts, which regulates the speed of the centrifuges in the enrichment program. The cyber worm made these software systems command the equipment to speed in a destructive manner, leading to the centrifuges destroying themselves.



In addition to propagation capabilities, many other advanced features are found:

- Stuxnet is able to mask itself from users on Windows machines and portable drives.
- It is able to connect to a command server for version updates and usage statistics (the two servers, originally located in Malaysia and Denmark, have since been rerouted to disconnect the Stuxnet operators).
- Infected computers on the same local network can update each other to the newest locally available version.
- Four previously unknown Windows vulnerabilities ("zero-day exploits") are used, an unheard-of amount for a single malware program.
- Two stolen digitally-signed certificates (for passing through virus protection software) were employed. The close proximity of the offices of the certificates' true owners suggests the possibility of an in-person theft of the files.

Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack; a link file that automatically executes the propagated copies of the worm; and
a rootkit component responsible for hiding all malicious files and processes, to prevent detection of Stuxnet. It is typically introduced to the target environment via an infected USB flash drive, thus crossing any air gap. The worm then propagates across the network,

scanning for Siemens Step7 software on computers controlling a PLC. In the absence of either criterion, Stuxnet becomes dormant inside the computer. If both the conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the code and giving unexpected commands to the PLC while returning a loop of normal operation system values back to the users.

INTRODUCTION

Cyber threats to critical infrastructure are real and actively evolving. Incidents at nuclear highlight the importance of developing and implementing rigorous regulatory frameworks, risk-based assessments, and improved digital protection capabilities.

As global nuclear energy grows, so does the threat of cyber attack. Over time, process control systems in nuclear power plants have evolved from early analogue systems to digital systems. Digital systems themselves are continuing to evolve from highly specialized hardware and software to more standardized hardware and software in Supervisory Control and Data Acquisition (SCADA) systems. The transition to digital systems brings with it new risks and vulnerability to new interconnects of system components, potential operational issues, and vulnerabilities from cyber-attack that must be assessed and addressed.

METHODOLOGY AND ASSUMPTIONS

ASSUMPTIONS:

- The power plant uses Cyber Physical System (CPSs) with main components SCADA, DCS and PLC.
- The PLCs are controlled by computers with Siemens SIMATIC WinCC/Step 7 controller software.
- Internal hard drive in a computer and/or USB storage devices are acceptable ways for staff to do their work.
- The process control network (PCN) and control system network (CSN) are hosted in the same security zone.

- The nuclear facility is located away from the central hub and professionals. It is required that a proper security system is established.

METHODOLOGY:

In protection against a cyberattack, four main categories of digital computer and communication systems must be considered:

1. Safety-related and important-to-safety functions
2. Security functions
3. Emergency preparedness functions
4. Support systems and equipment important to safety and security

SOLUTIONS

(1) Zero-Trust approach:

Assume all users, devices and software, both inside and outside your network, are insecure. Require strict and constant identity verification to access any resources within your network, and only grant access to those who need those resources to perform their job.

(2) Segmentation and Air-Gapped backups:

When there is an attack segmenting the network and air gapping the backups keep the ransomware from spreading and attackers from gaining a foothold into the rest of the systems.

The former isolates individual workloads within the network, protecting traffic traveling east-west within a data center, while the latter keeps the backups separate and secure even if ransomware begins spreading across the network.

(3) Unidirectional Security Gateways:

One solution for allowing network communication while minimizing risk is the use of unidirectional security gateways. These devices behave like a one-way firewall, allowing data to flow from allowed sending devices on one network to one or more receiving devices on another network.

(4) Encryption:

The use of encryption for storage media is an inexpensive method for securing data. Microsoft provides full-disk encryption known as BitLocker for Windows 7 and Windows 8. BitLocker provides either 128-bit or 256-bit AES encryption, and on systems with a supported TPM chip further security measures are available for key storage (Microsoft, 2012). Another option is to use properly vetted free and open-source encryption software such as TrueCrypt, which has been approved by cryptography expert Bruce Schneier. TrueCrypt has a wide variety of choices for encryption methods including AES, Twofish, and Serpent algorithms

(5) SIEM:

This software allows security teams to gain attacker insights with threat rules derived from insight into attacker tactics, techniques and procedures (TTPs) and known indicators of compromise (IOC)s. To do this it uses multiple threat intelligence feeds (organized and analyzed information on potential and current threats) which supplements threat detection.

Once SIEM software determines a threat, vulnerability, attack or suspicious behavior it creates alerts for the organization’s security teams for prompt response.

(6) IDS:

IDS identifies entities attempting to subvert in place security controls. An IDS uses integrated intrusion signatures for identifying potential malicious activities capable of damaging the network.

Host-Based IDS (HIDS): Deployed on a particular endpoint and protects it against internal and external threats.

Network-Based IDS (NIDS): Network-based IDS solution monitors an entire protected network. It has visibility into all traffic flowing through the network and makes determinations based upon packet metadata and contents.

(7) ICS SCMS:

- ICS Source Code Control and Management Systems provides a centralized location and repository for programming code including live production as well as development. In addition, versioning allows for the review of all changes made to code over time as well as to move back to the last known good version in case of unexpected errors.
- Rockwell Automation is an SCMS provider. Rockwell Asset Centre can be used as SCMS. Main features include a source control i.e., a centralized database that allows automatic version control, ability to perform automated backup, centrally schedule manage, track and report calibration activities enabling compliance to regulatory guidelines, etc.

(8) The fundamentals:

Many breaches occur not because hackers were able to pick the locks but because the doors were left wide open.
In other words, what might seem like the most basic security measures can go a long way to keeping attackers out.
Switch up the default login credentials on every device and schedule regular changes. Require employees to use strong passwords. Enforce multi-factor authentication (MFA).
Encrypt your data at rest and in flight. Keep up
with firmware updates and software patches.

CYBER DETTERENCE CHALLENGES

- ### Introduction to deterrence theory

Deterrence is: ‘a strategy intended to dissuade an adversary from taking an action not yet started, or to prevent them from doing something that another state desires', or 'dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit' This consideration should occur in the adversary's mind. Due to its rather abstract nature, making an analogy to the Cold War era's nuclear deterrence posture has been useful to provide a solid reference to discuss this phenomenon. In the nuclear weapons context, deterrence was achieved due to the weapons' immense destructive power. Use of these weapons would cause the targeted nation to respond in kind due to the long transit time of the warhead providing defender the opportunity to counterattack (Second strike chance). This fact negates any possible gain by either nation. The concept of mutually assured destruction rendered any plan involving a decisive first-strike nonsensical. This characteristic is quite different from the instant nature of cyberattacks.

CHALLENGES:

- ### Attribution:

Now that we have a basic definition of deterrence and the attributes necessary for success, the next step is to look at the challenges associated with applying those principles to cyberspace. One of the biggest barriers to effective cyber deterrence is the concept of attribution. Intelligence expert Bob Gourley maintains that "you cannot deter unless you can punish, and you cannot effectively punish unless you have attribution." Attribution in the cyber domain is possible, but in some circumstances it can be difficult and time-consuming. The complex structure of the Internet, immature political and legal policies, and global nature of the cyber domain make operating anonymously possible. Adversaries can exploit any number of system or protocol vulnerabilities to hide or spoof their location and can operate from nearly any physical location. The more sophisticated the attacker, the more difficult attribution becomes. These attackers will take actions to hide their true location and make it appear that another attacker or nation-state may have conducted the attack. Additionally, legal and political hurdles may make attribution difficult and time-consuming— especially when international cooperation among multiple organizations, agencies, and governments is required to determine the source of an attack.

- Understanding Adversary Motives and Level of Risk Tolerance:

Another challenge to cyber deterrence is understanding the adversary and how it will react to a given deterrence strategy. Cyber threats can be categorized in many ways, and each category will have different motivations and levels of cyber skills or capabilities. Our ability to deter each group of cyber adversaries will vary. For this paper, I group threats into the three categories of criminal actors, violent nonstate actors, and state or state-sponsored actors. Cyber-criminal activity is the largest group of cyber threats and one of the most difficult to effectively deter. This group of hackers ranges in sophistication from low ability (i.e., script kiddies) to elite-level hackers motivated by financial gain. Our ability to punish and deter this group is sometimes limited and largely dependent on law enforcement and effective cooperation from foreign nations. Sophisticated hackers will seek out places where governance and policy conditions facilitate masking their identities. Punishing this group can be complex for several reasons. First, as discussed, accurately attributing the source of cyberattacks is problematic and sometimes time-consuming. Second, the sheer volume of activity makes prosecuting all cases impractical. According to a 2013 US Government Accountability Office report on cybersecurity, the number of computer security incidents that federal agencies reported to the United States Computer Emergency Readiness Team (US-CERT) over a six-year period increased from 5,503 in 2006 to 48,562 in 2012 (a 782 percent increase). According to the Internet Crime Complaint Center’s 2010 Internet Crime Report, the Federal Bureau of Investigation received 303,809 Internet crime complaints resulting in 1,420 prepared criminal cases—which led to a mere six convictions

LEAGAL AND TREATY

Cyberattacks pose a growing threat to the integrity of sectors that are critical to our economic and social well-being. Cybersecurity threats have increased by over 358% in recent years, outpacing societies' ability to effectively prevent or respond to them. There is an urgent need for cooperation between government and business leaders to align global cyber regulations that safeguard data and privacy.

To create a cyber-secure world, we must be as fast and globally integrated as the criminals. Facing a global threat with local resources will not be enough. Countries need to do more internally and internationally to coordinate their efforts.

However, global cybersecurity and privacy regulations – while well-intentioned and seeking to contribute positively to the daily onslaught of emerging cyber threats – give limited consideration to harmonization between countries. The result, unfortunately, is discordant and confusing, like each section of an orchestra playing in a different key.

There are three areas where global harmonization of cybersecurity regulations could make us safer and enhance our access to innovative products and services:

1) Developing Consistent and Enhanced data protection

- Global standards ensure a common understanding of requirements rather than jurisdictional interpretations of law.
- Consistent application of data protection methods and procedures reduces risk and builds trust across borders and supply chains.

- Data duplication can be minimised by having fewer national data residency laws – less data proliferation means lower risk of data compromise.

2) Increasing Innovation and Interoperability

- Global inclusion is fostered when technical hurdles are lowered, allowing more interoperability.
- Inclusion feeds innovation by engaging the great minds and entrepreneurs around the world to participate in the global technological ecosystem.
- Interoperable architectures enable and facilitate privacy and security by design.

3) Reducing Cost

- Alignment with global standards will reduce the complexity of implementing security and privacy controls.
- Compliance exams could be streamlined through standard artifacts that meet the needs of all interested parties.
- The need for costly data residency requirements driven by security or privacy will be lessened.

- ### The Convention on Cybercrime or the Budapest Convention, 2001

The Convention on Cybercrime or the Budapest Convention is the first international treaty which seeks to address the issue of Cyber Crime. It was drafted by the Council of Europe along with active participation of Canada, Japan, South Africa and the United States of America. It is the only legally binding international instrument on this issue. It was opened for signature in Budapest from 23 November 2001 and it entered into force on 1 July 2004. The convention was formed with an aim to harmonize national laws, improving investigative techniques, and increasing cooperation among nations. It acts as a guideline for any state developing national legislation against cybercrime. India has not adopted the convention and declined to ratify it as it was not a participant in its drafting.

- ### Internet Corporation for Assigned Names and Numbers (ICANN)

It is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

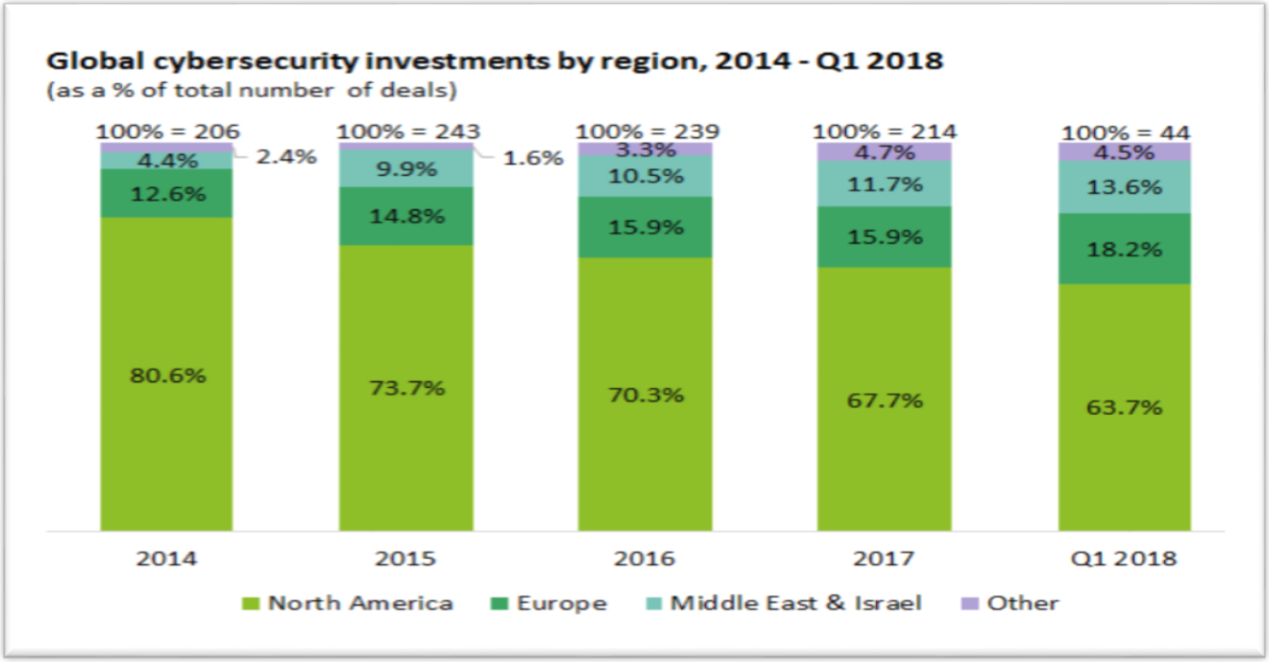
- ### International Telecommunication Union (ITU)

UN , to ensure connectivity in communication networks around the globe, established a body which would facilitate international connectivity in communications networks, develop the technical standards that ensure networks and technologies seamlessly interconnect and strive to improve access to ICTs to underserved communities worldwide, thus International Telecommunication Union (ITU) came into picture.

CYBERSECURITY INVESTMENT AROUND THE WORLD

The U.S. government spends $19 billion per year on cyber-security but warns that cyber-attacks continue to evolve at a rapid pace. The rising tide of cybercrime has pushed information security spending to more than $86.4 billion in 2017.

But in India, two out of three companies spend less than 5% of their IT budget for beefing up their cyber security.



BENCHMARKS OF SUCCESS

Cybersecurity never sits still. While you may have created a program that addresses the current cyber threats towards your organization, the chances are that it will not stay that way. New threats emerge, new techniques and technologies are put into play by cyber criminals.

PERFORMANCE METRICS:

The correct set of cybersecurity performance metrics will support the cybersecurity program, and help the organization make the right decisions when it comes to the future of the program. Tracking cybersecurity performance metrics over time will give early warning when tools or controls are no longer effective, when new tools need to be considered, or when additional resources are needed.

Below are just some examples of the many metrics that can be used to create a balanced report that will benefit the cybersecurity program.

- **Average time to patch vulnerabilities** – When vendors release security updates, how long does it take to update software? Delays to applying security patches leaves the organization open to cyber-attack through a known vulnerability. Best practice is to apply patches fast, and when patches are not available, to virtually patch in the interim.
- **Number of systems with known vulnerabilities** – Some systems may have known vulnerabilities. Knowing how many systems have known vulnerabilities, and what the vulnerabilities are in each system will enable your organization to manage risk.
- **Mean time to detection –** The longer it takes to detect attacks, the more damage attackers can cause. Average dwell time has dropped to 24 days, a significant improvement from 56 days in 2020, but it is still time for attackers to cause significant damage. The aim is to get as close to zero as possible.
- **Cost per incident** – Cyber incidents cost money, man hours, loss of productivity, and more. This cybersecurity performance metric will provide a picture of the resources used to clear up each incident. The aim is for this figure to be as low as possible.

SUCCESSFUL CYBERATTACK

Exercising command and control:

The attacker can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees.

the hacker can lock a company's IT users out of the organization's entire network if they want to, perhaps demanding a ransom to restore access designating a successful attack.

Achieving the hacker's objectives

Not all hackers are after monetizable data or incriminating emails that they can publish. Some simply want to cause chaos or to inflict pain on a company. Execution of the motives of the hacker is a sign of a successful cyberattack.

Sustainment:

After gaining access in the network, remaining undetected for longer time is also important to properly execute an attack. Rootkits can be installed in the victim's network to allow the attacker to enter and exit the network whenever he/she wants.

REFERENCES:

- https://acehacker.com/microsoft/cybersecurity/resources/Protecting_Critical_Infrastructure_Against_the_Next_Stuxnet.pdf
- https://acehacker.com/microsoft/cybersecurity/resources/Cyber-Security-Safeguarding-the-Networks.pdf
- https://acehacker.com/microsoft/cybersecurity/resources/After-Stuxnet-Acknowledging-the-Cyber-Threat-to-Nuclear-Facilities.pdf
- https://www.techopedia.com/4-ways-to-improve-your-critical-infrastructure-security/2/34765
- https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/
- https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html?sh=592c424951e8
- https://acehacker.com/microsoft/cybersecurity/resources/The-History-of-Stuxnet.pdf
- https://en.wikipedia.org/wiki/Convention_on_Cybercrime#:~:text=The%20Convention%20on%20Cybercrime%2C%20also,and%20increasing%20cooperation%20among%20nations.
- https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet
- https://www.sciencedirect.com/science/article/pii/S0267364910000506
- https://www.jstor.org/stable/pdf/resrep13817.9.pdf