PREVENTING STUXNET LIKE ATTACK OF INDIAN SOIL

BY ARYAN MAURYA

ABSTRACT

Critical infrastructure protection is vital to the day-to-day operation of any country, and those systems need to be protected to the fullest extent possible. Cyber security can be referred to as the protection of data and systems in networks, both wired and wireless, from unauthorized access or attack. Having an advanced nuclear system is important for national security. Hence, countries are spending billions of dollars for gaining momentum in their nuclear plans. But as nuclear power is proving to be authoritative, the nuclear system is becoming prone to cyber-attacks. Over the past twenty years, five deadly cyberattacks compromised the national security in five countries. Not only affecting the internal security of any country, but cyberattacks have proven perilous for the privacy of the citizens. As new technological innovations are permeating the industry, the incidence of security breaches and possibility of cyberattacks has heightened. That's why scaling-up cybersecurity in nuclear institutes and models, become important.A cybersecurity breach has several implications. Due to a cyber malware, the confidential documents associated with cyber security can be leaked. It can increase the vulnerabilities of nuclear systems. With a disrupted nuclear system, the adversaries can take advantage by corrupting the communication, and preventing the flow of information. Moreover, cyber-attacks are a direct threat to the integrity of any nation.

In September 2019, the cyber attack at Kudankulam Nuclear Power Plant only exposed the dearth of cyber-security management in India. The attack was caused by the DTRACK Virus, which was developed by a group of hackers from North Korea. It was a direct attack on the administrative framework of India and was confirmed by ISRO. The confidentiality of a large amount of data was threatened due to this attack. In nuclear power plants, assessments of cyber security are critical to ensuring the safe and reliable operation of the systems used. And the biggest threat today is STUXNET. The Stuxnet virus set off alarm bells all over the world when it was discovered in 2010. Many observers viewed this unprecedented cyber attack on a nuclear facility as the dawn of the age of cyber war -"the keystroke heard 'round the world." Stuxnet also had significant implications for nuclear security. The attack revealed a troubling reality: in the future, cyber weapons could be used against nuclear facilities to achieve consequences far more serious than those observed at the Natanz uranium enrichment facility in Iran. Stuxnet was an extremely precise weapon deployed against a highly secure facility for a very limited purpose. At no point were human lives or the environment in danger. However, this will not always be the case. With the code for Stuxnet now widely available online, it may only be a matter of time before a group intending to cause harm deploys a less discriminate weapon against a less secure, higher-consequence target like a nuclear power plant or nuclear materials storage facility.

INTRODUCTION

Throughout late 2009 and 2010, centrifuges spinning in Iran's Natanz uranium enrichment facility started to break at unusually high rates. In time, it would become clear that these disruptions were not standard mechanical failures; they were the result of Stuxnet, a cyber weapon designed and deployed with the goal of slowing or halting Iranian uranium enrichment. Stuxnet is a computer worm, that is, a virus with the ability to copy itself and travel quickly between computers. It was crafted to quietly take over industrial control systems and break the fragile, antiquated IR-1 centrifuges spinning at Natanz. Natanz's technology is widely viewed by the international community to be critical to Iran's pursuit of nuclear weapons. Revelations about Stuxnet opened eyes in countries all over the globe. This was the first instanceof a targeted cyber attack causing physical damage to highly sensitive infrastructure. Many observers viewed this discovery as "the keystroke heard 'round the world"—effectively, the dawn of the age of cyber warfare. Examining Stuxnet in a larger context, however, also reveals a troubling gap in the advancements made in nuclear security over the past decade.Nuclear facilities around the world remain too vulnerable to cyber attacks that could facilitate the theft of nuclear material or a radiological release. Stuxnet, the code for which is now available to anyone with Internet access and sufficient funds, was able to penetrate a highly secure facility and cause physical damage intended to be limited in scope.

This paper will highlight the challenges faced by ICS and nuclear facility in general and suggest the solutions to prevent cyber attacks.

METHODOLOGY

PROTECTING A NUCLEAR POWER PLANT

ACCORDING TO CNII GLOBAL POWER AND UTILITY SECTOR REMAINS THE MOST TARGETTED SECTOR TO CYBER ATTACKS.SINCE THE STUXNET ATTCAK OF NATANZ NUVCLEAR FACILITY THERE IS AN ENORMOUS NEED TO DEVELOP A SOLOUTION TO PROTECT NUCLEAR FACILITIES FROM SUCH ATTACKS

ASSUMPTIONS

CPS(CYBER PHYSICAL SYSTEMS) USING SCADA SYSTEMS ARE USED IN NUCLEAR FACILITIES AND MANY INDUSTRIES AS ICS. AND THEY ARE PRONE TO ATTACKS HENCE NEED TO BE PROPERLY PROTECTED

WITH THE NUCLEAR FACILITY LOCATED AWAY FROM THE CENTRAL HUB AND PROFESSIONALS IT IS REQUIRED THAT A PROPER SECURITY SYSTEM IS ESTABLISHED.

IDS AND FIREWALLS WILL BE INSTALLED ON EACH AND EVERY SYSTEM ON THE NETWORK ASSUMING ALL THE RESOURCES,MONEY AND LICENSES AND PROPER IT PROFFESIONALS TO CONFIGURE THEM PROPERLY.

CLOUD STORAGE IS NOT USED AND PORTABLE DEVICES FOR TAKING BACKUPS ARE USED

NO LIMIT ON RESOURCES ,MANPOWER AND IT PROFESSIONALS.

CPS SYSTEMS

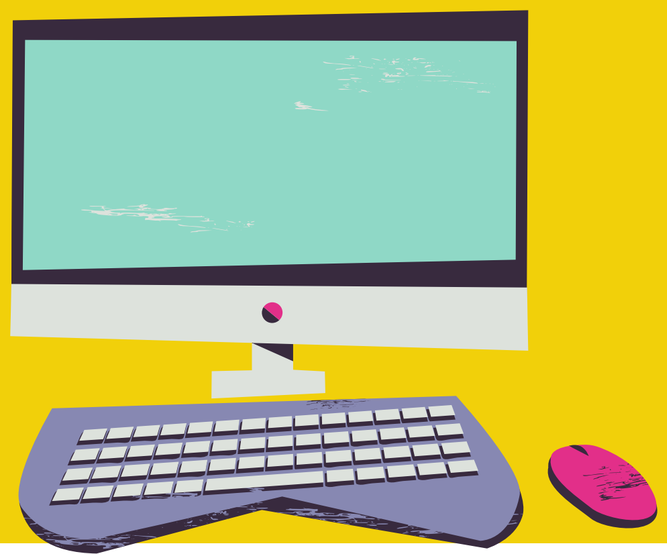
WHAT IS A CPS?

- *CPS system is a system that provides control over industrial components througfh cyber based commands .It is a physical system whose operations are being monitored ,integrated and controlled by a computational core.*
- *CPS represents a high level coordination between physical and computer elemnts.*
- *Industrial Control Systems(ICS) are CPS and used at industrial level.*
- *the main components of CPS are SCADA,DCS and PLC.*

1)SCADA

- *Supervisory Control and Data Acquisition(SCADA).*
- *Main role of SCADA is to gatherand control the assets distributed at different geographical locations .*
- *Gather data in real time from different locations in order to control equipment and conditions.*
- *Helps maintain efficiency by collecting and processing real-time data. SCADA is a centralized system that monitors and controls the entire area.*

CPS SYSTEMS



2)DCS

- *Distributed Control System(DCS)*
- *Controls the controllers that are grouped together to carry out a specific task located at a particular location.*
- *Handles the different assets that are p[art of SCAD.Platform for automated control and operation of ICS.*

3)PLC

- *Program Logic Controller (PLC)*
- *Small industrial computers with modular components designed to automate customized control processes.*
- *Both SCADA and DCS use PLC devices to control components and processes.*

LEGAL AND TREATY ASSUMPTIONS

TREATY ASSUMPTIONS

- *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.*
- *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.*

TREATIES

- *1)---In an increasingly digital world with sophisticated cyber threats Quad recognizes an urgent need to take a collective approach to enhancing cybersecurity.To deliver on the Quad Leaders vision for a free and open Indo-Pacific, Quad commits to improving the defense of member nations critical infrastructure by sharing threat information, identifying and evaluating potential risks in supply chains for digitally enabled products and services, and aligning baseline software security standards for government procurement, leveraging our collective purchasing power to improve the broader software development ecosystem so that all users can benefit.*
- *The Quad also plans to create a Quad Cybersecurity Partnership. They will coordinate "capacity building programs" within the region and launch a Quad Cybersecurity Day to "help individual Internet users across our nations, the Indo-Pacific region, and beyond to better protect themselves from cyber threats."*
- 2)----A new MoU was signed between Australia and India in April 2017, focusing on combating terrorism and civil aviation security. Cybersecurity cooperation is mentioned in the MoU.
- 3)A preexisting MoU between France and India was added to the mapping, signed in January of 2016. Officials of both countries agreed to intensify cooperation between the Indian and French security forces in the fields of homeland security, cyber security, Special Forces and intelligence sharing to fight against criminal networks and tackle the common threat of terrorism.

TREATIES

- *4)---A preexisting MoU between Singapore and India was added to the mapping. The MoU was signed in January 2016, focusing on the establishment of a formal framework for professional dialogue, CERT-CERT related cooperation for operational readiness and response, collaboration on cyber security technology and research related to smart technologies, exchange of best practices, and professional exchanges of human resource development.*
- *5)---A new MoU between India and the US was signed in March 2017. CERT-In and CERT-US signed a MoU agreeing to promote closer co-operation and exchange of information pertaining to cyber security in accordance with relevant laws, rules and regulations and on the basis of equality, reciprocity and mutual benefit.*
- *Considering the treaties with different nations it is safe to assume that the allies ,friendly nations would assist the organization if needed in terms of materials,man power ,third party assistance,not revealing the information sharing with any other client unless needed ,manpower etc.*
- *In case of any incident in organization ,it can be assumed that the nations would provide full assistance during retaliation in case the attacker/attacker organization is from their country and also provide assistance in tracking down the attacker if not from their country.*

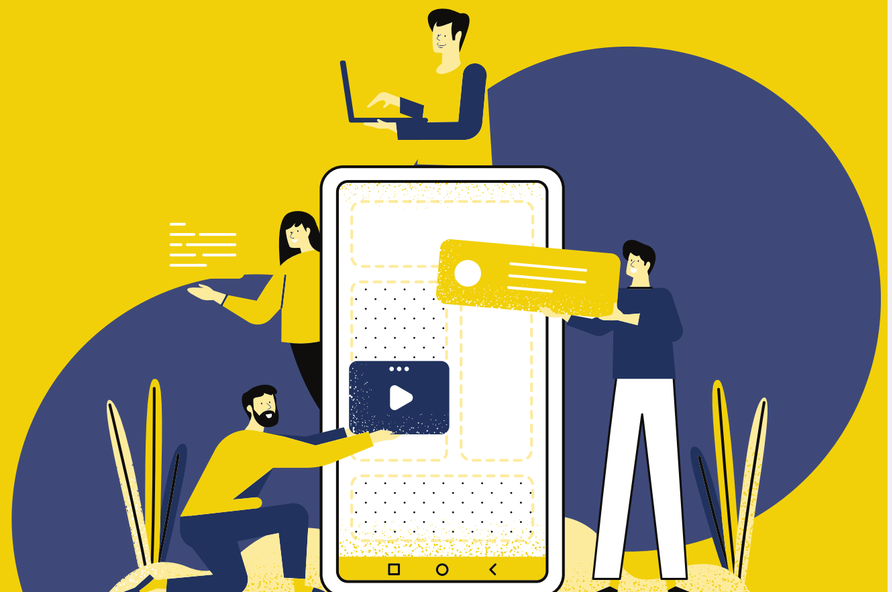
CHALLENGES

CYBER CHALLENGES

PORTABLE DEVICES

- *For ICS systems especially those in nuclear facilities with air gapped control systems,portable media is one the the only ways of moving data between seperate networks.*
- *Routine operations like taking backup of the data,installing software upgrades or patches,installing OS upgrades are done through portable media.*
- *Stuxnet was believed to be introduced through a USB into the network hence to insure that none of the portable storage media do not contain any malicious program is a significant challenge*
- *Stuxnet exploited zero day vulnerability hence it is a significant challenge to come up with methods to protect the system from risks that come due to use of portable media*

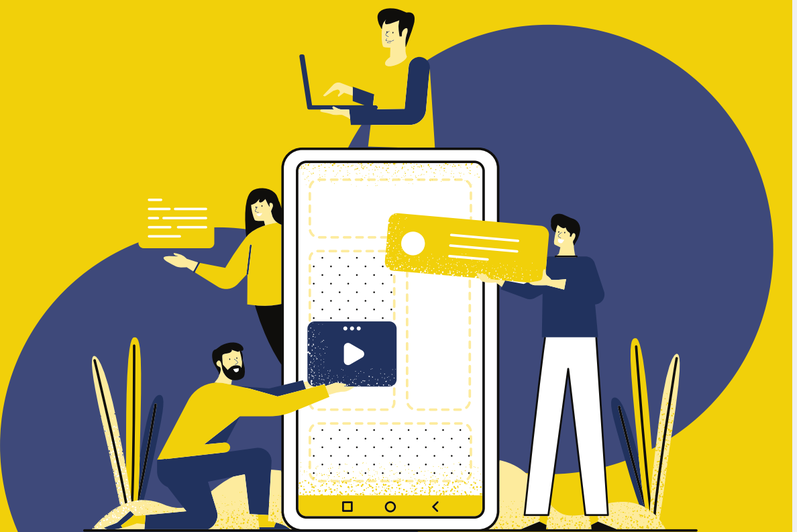
CYBER CHALLENGES



SIZE AND COMPLEXITY OF CPS(CYBER PHYSICAL SYSTEMS)

- *CPS(cyber physical sysetms) consists of the scada(supervisory control and data acquisition),DCS(distributed control system) and PLC(program logic controller) ard are used to operate Industriial Control Systems.*
- *In CPS there exists networking between different components of the systems to provide efficient and better reults in operation.In a network where all nodes are trusted there every component can be a point of attack .Hence as the complexity and size of the CPS increases the entry points for attackers increase.*
- *Often in complex CPS ,securing the servers and SCADA overshadows the security of components of low level importance which can be used by the attackers as an entry point.*
- *Identifying the critical control points and component interactions that effect those points is important but as CPS gets more and more complex it becomes more difficult to anaylse it completely and we may leve certain components vulnerable to attacks.*

CYBER CHALLENGES



LACK OF COMMUNICATION AND KNOWLEDGE

- *Governments and nuclear facilities do not diclose the incidents that occur due to concern for reputation and trust among other countries.*
- *Nuclear Personnel often consider cyber incidents as malfunctioning of hardware due to lack of nuclear forensics to determine cause of incidents./*
- *Nuclear plant personnel have a hard time communicating their security requirements and suggestion which might be duye to off site location of cyber professionals and lack of awareness among personnel.*
- *Level of technical training is insufficient .Many employees leave their PC unatttended with their personal emails,softwares and senstive documents running .A single mistake could lead to a cyber accident.*
- *A lot of times eve the default passwords are not changed which might help the attacker to penetrate easily into the network.*

CYBER CHALLENGES

INTERNET CONNECTIVITY

- *Nuclear Facilities nowadays require internet connectivity because third parties such as owner-operators,vendors and head officers are located off site and need access to the data generated at the plant.*
- *Data is required to update the deployed software ,check the plant status and rapidly daignose the malfunctions occuring at the plant.*
- *malware can be sent through these systems by bypassing the mechanisms of IDS and Firewalls installed in case the basic rules are being used in them..*
- *Incoorectly configured VPN coulkd also lead to an attack .*
- *SCADA systems use TCP/IP protocol which are known to have vulnerabilities like IP Spoofing,amn in the middle attcaks ,SQL Injection etc.*

CYBER CHALLENGES

AVAILABILTY OF MALICIOUS CODE

- *Existence of stuxnet code online has enabled attackers to develop and modify it to their own destructive purposes.*
- *Increase of penetration testing and exploitation tools like Metasploit are being used used by attackers to execute malicious payload on systems.*
- *Companies in grey markets may also sell unknown zero day vulnerabilities to nation states / non state hackers.*

CYBER CHALLENGES

COUNTER RETALIATION CHALLENGES

- *Cybersecurity requires having the initiative in anticipating exploitation of vulnerabilities. During retaliation, we have somewhere ceded the initiative to an adversary, who was able to exploit something before we could anticipate that exploitation. Thus, we become more insecure.*
- *Retaliation also poses the risk of waging a cyber war against a nation state if the attacker is idneed a nation state.There are legal issues involved in retaliation to cyber attack which can be violated causing further damage.*
- *Retaliation makes our system more insecure and might invite other attackers to attack also the previous adversary also now has an idea about our netowrk hence will have lesser problem in going after us in counter retaliation and even multiple adversaries might unite during counter retaliation thus causing more harm than previously.*
- *In Retaliation we might expose our technologies to the outside world which might develop resistance to it as a counter and further prepare themselves for another attack.*

CYBER CHALLENGES-RISKS

CYBER ESPIONAGE ,CYBER ATTACKS/TERRORISM AND CYBER SABOTAGE

- *CYBER ESPIONAGE-Use of malware like spyware and key loggers to penetrate a trusted network an access senstive information,Duqu ,zeus and malwares by DeepPanda have been used to gain intelligence from critical infrastructure .*
- *CYBER TERRORISM-Stuxnet was not meant for causing loss of life but to disrupt the working of centrigfuges in Natanz facillity in Iran.However an attcaker can tamper with reactor control systems,potentially leading to radiological release causing damage to life.Terrorist groups may use the vulnerabilities in ICS systems of nuclear facilities to trigger an attack.*
- *CYBER SABOTAGE-Physical disruption to the nuclear equipment and components of the ICS ,introduction of malware and other viruses or even planting malware that can result in an explosion.The third parties and vendors for these facilities are also threatened..*

CYBER CHALLENGES-RISKS

POSSIBLE MEANS OF ATTACKS

MALWARE---

- *1)Worms*
- *2)Viruses*
- *3)Trojen Horses-RAT(Remote Access Trojan) can be used to take control of the ICS system and control it.*
- *4)RootKIt Attacks (extremely Dangerous)*

- *DDos Attacks*
- *SQL Injection(discussed before),Session Hijacking*
- *Social Engineering attacks.*

CYBER CHALLENGES

POSSIBLE MEANS OF ATTACKS

MALWARE---

- *1)Worms*
- *2)Viruses*
- *3)Trojen Horses-RAT(Remote Access Trojan) can be used to take control of the ICS system and control it.*
- *4)RootKIt Attacks (extremely Dangerous)*

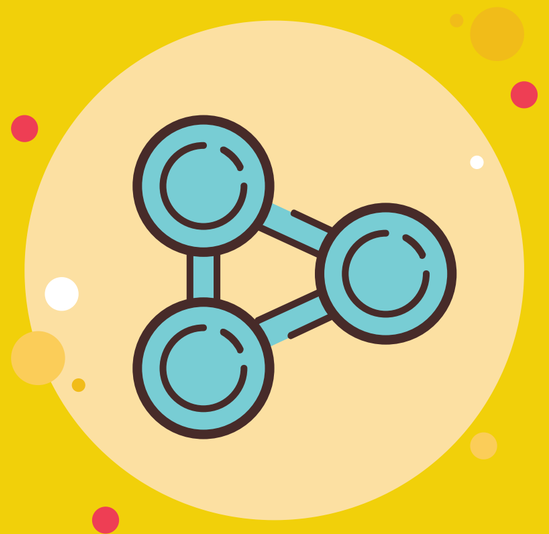
- *DDos Attacks*
- *SQL Injection(discussed before),Session Hijacking*
- *Social Engineering attacks.*

SOLUTION

TRAINING AWARENESS AND EDUCATION

- *Training equips individuals with the necessary skills to perform specific functions within the organisation. Employees must be made aware of information.Security policies and the importance of adhering to them. Communicating this to all employees is vital to ensure they know, understand and comply. The key outcome of security awareness programs and activities is to create a culture of security, change of behaviour and attitude.*
- *Careless attitude towards cybersecurity is often the rootcause of problems thus equipping the personnel of the facility will help reducing the risk caused by the man factor.*
- *As the facilities are situated far away from central hub and IT Professionals hence crash couses and online propgrams on cyber security can be used to make the employess aware about cybersecurity and its need .*

INFORMATION SHARING , COOPERATION & LEGAL COMPLAINCE

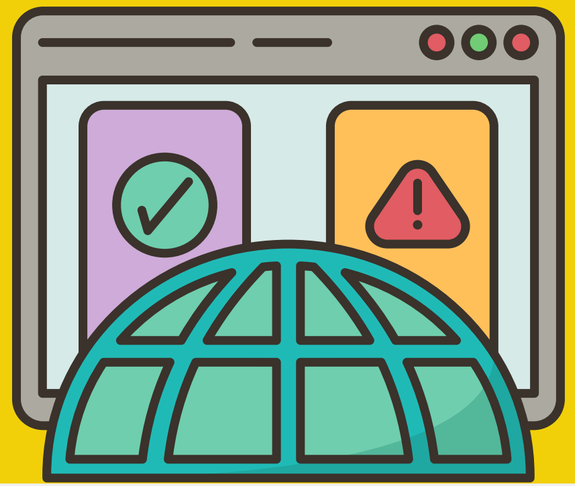


- *Through information sharing, the facility reduce and prevent the spread of the attack and minimise the damage to the infrastructure and country in large.Through partnerships, sectors can share information aswell as collaborate to solve issues relating tocybersecurity threats and attacks. Alliances also help to share skills within the sectorswhere some unique skills may be required from thegovernment or private sector.*
- *Legal compliance ensures that operators meet criticalsecurity standards identified by national decision makers.Although for ICS in Nuclear facilities the security standards will be very strong as needed.*

1)FIREWALLS

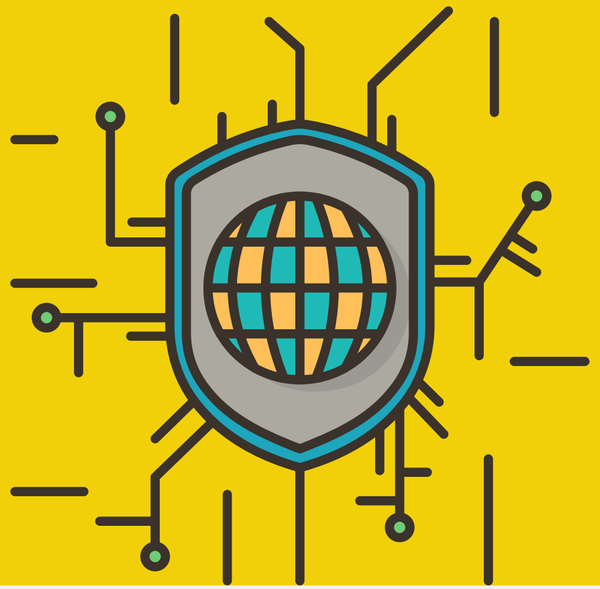
- *Before Moving onto a specific security system its important to secure the network and the computers connected to the network.*
- *ICS has a number of computers connnected to a network hence it is important to protect each one of them .*
- *A Network based ,Stateful,Hardware Firewall needs to be install in ICS.*
- *The incoming traffic needs to be correctly treated so that any malicious code is not passsed through firewall hence all the trafic needs to be analyzed hence a stateful firewall is needed.*
- *Multiple computers will operate on the network hence a network based firewall is needeed thus applying the same configuration on all computers.*
- *Since a lot of traffic will be analyzed as ICS has a very large network hence Hardware firewall is required which increases bandwidth and capable of handling more packets per second..Supports VPN and encryption hence protecting ICS hence is less prone to cyber attacks..*
- ***DMZ ZONE**- ICS require DMZ zones as it protects the internal of network from untrusted traffic(the external network) thus a DMZ needs to be established in the firewall.*

2)IDS



- *Stuxnet caused a deviation from the normal control and working .IDS looks for intrusions in the network.Any Attack on nuclear facilities would try to disrupt the working mainly like cyber terrorism and cyber sabotage as in case of Stuxnet.*
- *Hence an IDS based on anomalities would be the better opytion for ICS in Nuclear facilitries.Such IDS builds what is normal in the network and if a deviation from normal working or abnormal amount of traffic is detected then it raises an alarm.*
- *As the entry point for attack can be any single computer hence all computers need to be protected .Host Based IDS are a better choice as it scans a particular computer for malicious programs and monitors its functionality.Network IDS wont be able to detect if an attcaker is sitting locally.*
- *All computers connected to the newtork to be acquipped with Host Based IDS.*
- *SNORT can be used as an IDS .It is open source IDS tool.*

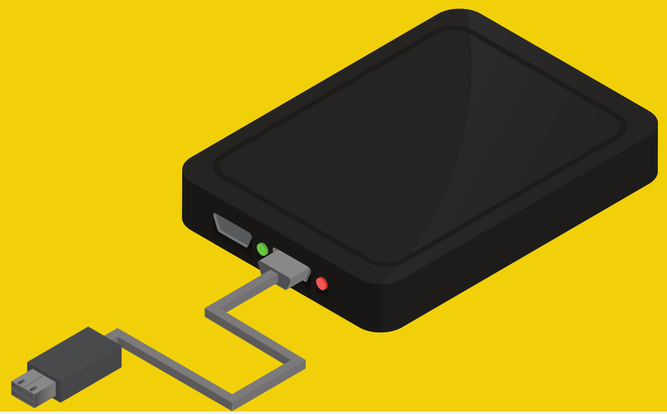
3)SIEM AND MALWARE ANALYSIS TOOLS



- *SIEM (Security Information and Event Management) tracks status of all the events in a computer .Detects if there exists a threat.If there is ,then categorizes if it is critical or not and thus applies coutermeasures to handle the threat.*
- *SIEM tools work by gathering event and log data created by host systems, applications and security devices, such as antivirus filters and firewalls, throughout a company's infrastructure and bringing that data together on a centralized platform. The SIEM tools identify and sort the data into such categories as successful and failed logins, malware activity and other likely malicious activity.Threat Recovery Stem is finally executed to revert back to the condition before attack..*
- *SIEM interacts with different applications hence analyse all the data and produces reports and graphs as output in real time on demand.*

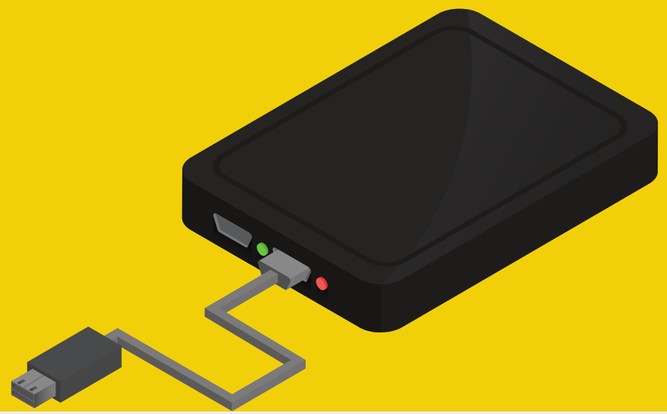
- *Malware have a specific signature assigned to them .Antivirus tools look for those signature in files to preotect device from malware.However malware can mutate themselves hence its not really an effective method.*
- *YARA-A simple tool that looks for sniffers(inspects traffic both incoming and outgoing).If sniffer is present in a file the it is handled accordingly.*

4)ENCRYPTION



- *Encryption should be used for senstive data including the storage of code,configuration information and files needed for production utility operations that must fucntion reliably .*
- *USe of encryption is an encryption is an expensive method for securing data.*
- *Microsoft provides full disk encryption known as BitLocker which provides a 128 but or 256 bit AES encryption on system with a supported TPM chip.Further security measures are available for key storage*

5)HANDLING PORTABLE DEVICES



- *Moving on to more specific safety propositions.The handling of portable devices in ICS is important as The Stuxnet virus is believed to be introduced into the system through the use of USB.*
- *USB are used in Industries to take regular backup band installing softwares uipgrades and patches,OS updates etc.*
- *One method is the use of WORM (write once read many) devices for taking backup.Example using DVD discs to store backup of data.Data assets stored on the computers in ICS can be burned to the DVD and those DVD to be placed at a safe location .*
- *Using a stand alone computer with boot-able operating system such as Knoppix Linux.This avoids the possibilty of using malware infected comuter for performing formatiing.The Computer with boot-able OS has to be installed with a trusted ISO image and booted using a USB that was also formatted fresh.*
- *Such computers minimize the risks from portable media*

6)UNIDIRECTIONAL GATEWAYS

- *Securing Networked Control Sytems requires a different approach.The ICS nowadays are connected to the network to contact to the vendors and other off site partners.*
- *Unidirectional Gateways minimize trhe risk to Networks ICS.These devices behave like a one way firewall allowing data to flow from allowed sending devices on one network to one or more recieving devices on other network.*
- *Such systems allows data to only move out from the ICS and nothing can go back in thus minimizing the chances of introduction of a malicious program/code into the network.*
- *Some Unidirectional Gateways providers are Waterways Security Solutions and RAD.*
- *Waterways Unidirectional Gateways-Uses a fire optic cable that is phyically able to send data only one way..Also offers complete cutomizable configuration of the application stack.*

7)ICS SCMS

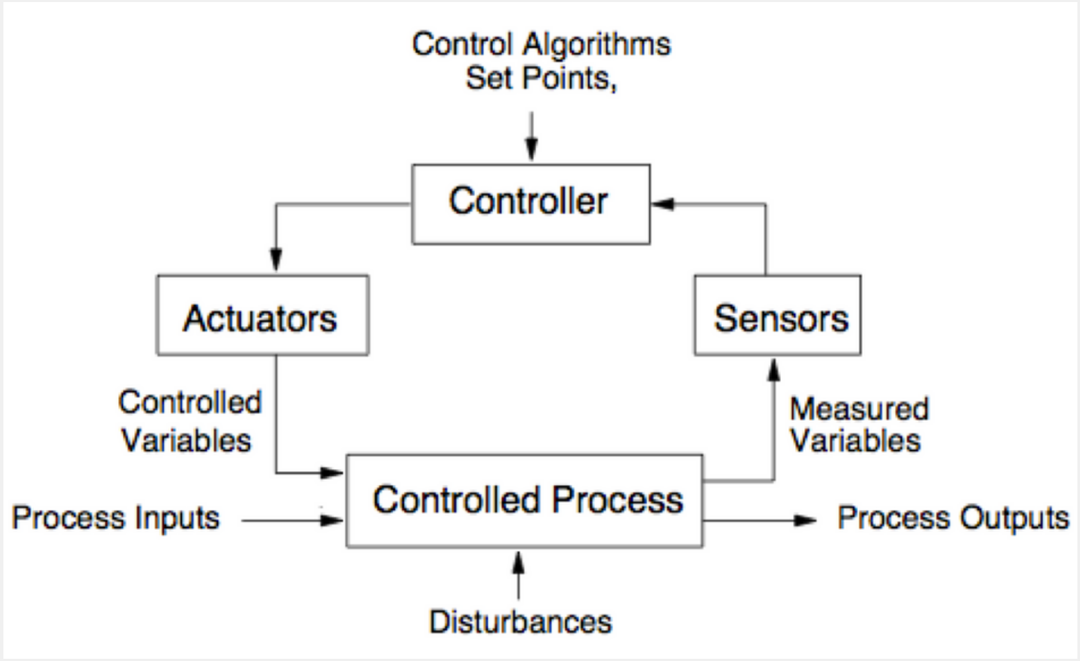
- *ICS Source Code Control and Management Systems provides a centralized location and repository for programming code including live production as well as development. In addition, versioning allows for the review of all changes made to code over time as well as to move back to the last known good version in case of unexpected errors.*
- *Rockwell Atutomation is an SCMS provider.Rockwell Asset Centre can be used as an 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 callibratio activities enabling compliance to regulatory guidelines etc.*

8)STAMP MODEL

- *Now coming to the model that will be used to cover the entire system all at once --- STAMP(System Theoretical Accident Model and Process)*
- *STAMP looks at the system as a dynamic one rather than a static one. and considers safety and security as a control issue.*
- *Individula components of the system are controlled by specific constratints specified in the model.*
- *STAMP assumes that the inadequate enforcement of the required constraints at all levels including design and development of the system can lead to an accident.*
- *An accident in STAMP refers to any undesired events that lead to system failure without component failure or miss interactions among components.*
- *STAMP analyzes the hierarchical control structure by monitoring how the control structures in system at different levels interact to have a safe and secure state.*
- *STAMP{ also helps find mitigation of the detected unsafe state.Also STAMP allows to uncover the reason responsible for cyber,envioronmental and organizational failures.*

8)STAMP MODEL CONTINUED

- *STAMP uses three pillars known as 1)Safety control Structure 2)Safety Constraints and 3)Process Model.*
- *The safety control structure shows the hierarchy of all control loops in the system from higher levels to lower levels.*



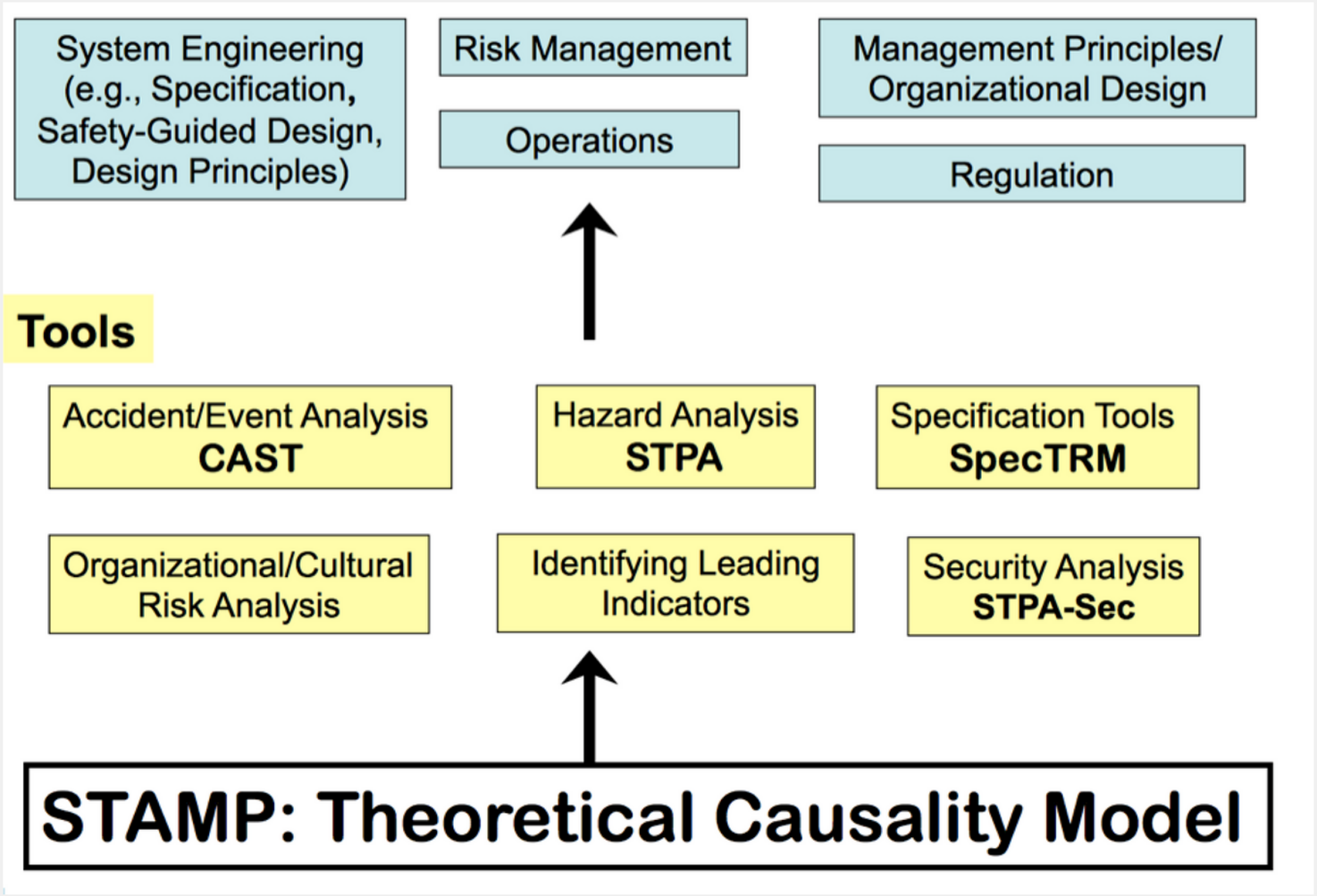
- *The above figure shows a simple control loop.*

8)STAMP MODEL CONTINUED

- *The main components of the simple control loop are-Controller, Actuators, Controlled Process, and Sensors.*
- *Controller receives a command from the operator or other controllers, it runs the control algorithm associated for the received commands. The result of this step generates a command signal that tells the actuator to change the state of the controlled process. Then, the actuator informs the controlled process that the requested command is executed by sending the related controlled variables.*
- *Finally, the sensors verify the system state using the measurement variables and sends the result back to the controller. At this point, the controller compare the system state with the desired state and determines the subsequent actions.*
- *The process model that is run by the controller confirms the controlled process results.*
- *Safety constraints are used to identify the safe and unsafe state of a system. They are derived from hazards that are defined in the system specifications. The successful design and enforcement of safety constraint increases system safety.*
- *In STAMP, these constraints are used to generate the system requirements that are mandatory to maintain the system safety. STAMP analysis not only shows where insufficient control action were in place but also shows which safety constraints were violated that brought the system to an unsafe state.*

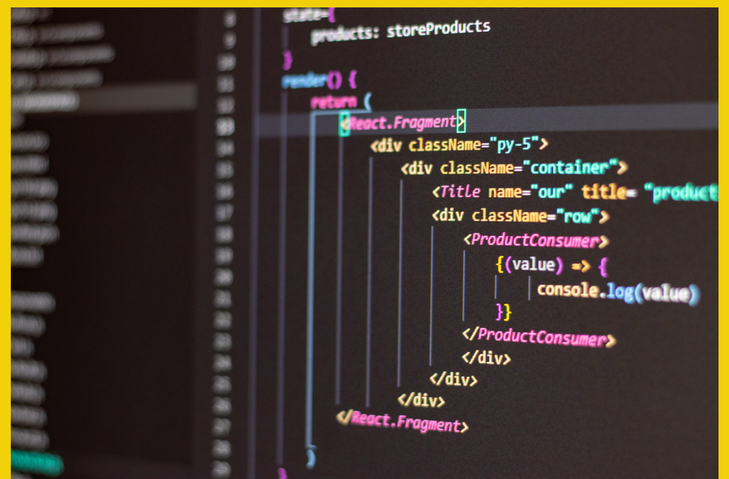
8)STAMP MODEL CONTINUED

- *STAMP methodology can be used both after an event to prevent future such events and before any such event to anticipate threats and mitigate them.*



PROTOTYPES

PROTOTYPES



- *The following prototypes are very basic highlighting basic IP tables rules for connecting ports,Blocking any traffic from particular IP address(or range of IPs).A simple port Scanner to scan a list of known ports from a particular host.*
- *A simple DNS exploration script to scan a domain and its subnomail and list what ever found and one very basic yara script.*
- *Link to the git hub repo is----*
- *https://github.com/aryanm17/Scripts_AryanMaurya17.git*

BENCHMARKS FOR SUCCESS

1)WHILE PROTECTING

PROTECTION METRICS

PROPORTION OF DEVICES WITH ENDPOINT PROTECTION

Endpoint refers to the computers ,srervers and other devices connected to the server.These devices need to be protected.In ICS this parameter needs to be fulfilled 100% to achieve best security standarsds that are very much required by the industry.

NUMBER OF USERS WITH SUPER USER OR ADMIN RIGHTS

Admin or super user accounts can be used in privilege escalation attacks. The principle of least privilege dictates that admin or super user rights should be given to as few people as possible in order to carry out their work. The number should be as low as possible.

AVERAGE TIME TO PATCH VULNERABILITIES

Delays in patching the vulnerabilities
leaves the ICS vulnerable to attacjks >the vulnerabilities needs to be patches as soon as possible in days or even hoyurs

CYBERSECURITY TRAINING SESSION RESULTS

Employees needs to be properly trained with security basics.Employees nbeed to be made properly aware of all the dangers that exist and must properly tell them the safety protocols that need to be followed to protect the ICS

PROTECTION METRICS

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 enablethe ICS to manage risk.

AVERAGE VENDOR SECURITY RATING

The vendors that are supplying security to the system must have hight rating .These ratings should be seen beforehand.The risk ratings for the third party used must be low

SECURITY POLICY COMPLIANCE

Security policies that are established at com panies and country level must be properly followed to avoid any legal issues.

BENCHMARKS FOR SUCCESS

2)UNDER ATTACK

INCIDENT METRICS

UNIDENTIFIED DEVICES ON THE NETWORK

The aim of this is to be as close as possible to zero – IT security should be able to identify every device on the main network.All the unidentified devices shall be identified

MEAN TIME TO DETECTION

The longer it takes to detect attacks, the more damage attackers can cause. Average time to detect the attcaks must be reduced . The aim is to get as close to zero as possible.

MEAN TIME TO RESOLUTION

The longer it takes to resolve a cybersecurity incident the more it will cost your organisation in downtime, reputation, customers, and money. The aim of this cybersecurity performance metric is to improve the response time to incident.

INCIDENT METRICS

REPORTED INCIDENTS

The number of incidents that are reported and detected by the monitoring tools should be properly highlighted and the rate of these incidents should decrease in effective security management system.

NUMBER OF INCIDENTS BY CATEGORY

It should also be noted that numebr of incidents by category should also be reported so that proper management can take place and so that after the incident vulnerabilities causing such incident can be patched.

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. These factors should be as low as possible

DOWNTIME

When systems are down then employess cant do their work and ICS especially nuclear facilities will face a huge problem as the plant wount be able to function and generate electricity for that much time.Hence the downtime should be as low as possible

BENCHMARKS FOR SUCCESS

3)PERFORMING ATTACK

BENCHMARKS

PROPER RECONNAISANCE

Reconnaisance refers to identifying the taerget and properly analyzing it.A successfull attack needs a proper recognition of the target.The organizational structure,vulnerabilities ,weak points etc shall be known of the victim to perform a successfull attack

SCANNING

Scanning of target network to identify entry points that allows to gain access of the network is important for an efficient attack.This process needs to be done carefully to exploit vulnerabilities .

ACCESS AND ESCALATION

Next step in the cyber attack is to gain access and then escalate to moving through the network undetected.Privileged access is needed because it allows the attackers to move freely within the environment. Rainbow tables and similar tools help to escalate privileges to admin, and then get into any system on the network that's accessible via the administrator account.

SUSTAINMENT

After gaining access in the network remaining undetected for longer time is also important to properly have an assault on the victim's network.Malicious program,RootKits are installed in the victim's network that allowes the attacker to enter into the system whenever required and leave when needed.

REFERENCES

01 https://www.information-age.com/7-steps-hackers-take-execute-successful-cyber-attack-123460872/

02 https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-how-retaliation-shapes-cyber-conflict/

03 https://blog.malwarebytes.com/security-world/2022/05/the-quad-commits-to-strengthening-cybersecurity-in-software-supply-chain-fronts/

04 https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016

05 After-Stuxnet-Acknowledging-the-Cyber-Threat-to-Nuclear-Facilities

06 A-Systems-Theoretic-Approach-to-the-Security-Threats-in-Cyber-Physical-Systems-Applied-to-Stuxnet

07 GW-CSPRI-2016-03+MASOOD+Rahat+Nuclear+Power+Plant+Cybersecurity_0

08 Protecting_Critical_Infrastructure_Against_the_Next_Stuxnet

THANK YOU