Research Paper

to

National Critical Information Infrastructure Protection Centre (NCIIPC)
Government of India

A Research Paper detailing how to prevent a Stuxnet like attack on Indian soil.

Praveen Singh
Microsoft Cybersecurity expert

Abstract

This paper discusses the possible cyber threat to the National Thermal Power Corporation(NTPC) gas-based power plant in Auraiya, Uttar Pradesh. The paper describes the potential problem caused by the current system in the facility and the solution architecture that can be implemented to prevent such a situation. The paper uses the Stuxnet attack on the Iranian nuclear enrichment facility in Natanz as a reference for modelling both the threat and the solution.

Table of Contents

Chapter 1

Introduction

Over the past decade, power plant control systems have evolved from DCS-centered platforms with proprietary software, to open systems using industry standard hardware and software, and then to totally integrated plant automation systems with almost unlimited connectivity and the ability to interrogate field instruments from many different manufacturers. What's next?[1]

The next here refers to more advancement in the technological fields for the power plant that will help automate and control most of the work along with collecting, monitoring and interpreting data. But with these advancements comes the risk of loopholes that a skilled group of hackers can manipulate for malicious purposes. We are now looking at one of the gas-based power plants of NTPC in Auraiya, Uttar Pradesh. The plant has six operational units totalling 652 MW capacity with 4x110 MW Gas Turbine and 2x106 MW Steam Turbine, having primary fuel as Natural gas.[2] The plant uses Cyber-Physical Systems(CPS) to automate most of the tasks, including real-time data collection and transmission, triggering actions at the process, sub-process, and device levels.

Chapter 2

Problem Statement

Since most of the operations in recent times are computerised, involving the triggering of various machine equipment at the process, sub-process and device level using IoT, it can be manipulated using the unpatched vulnerabilities in the software.

Most of the tracking, monitoring, alarming and data collection systems are all computerised, and access to the network can be used to easily manipulate them, so if the tech staff are working remotely(due to the new normal situation), then these data can be easily manipulated to trick them in believing that the situation is in control.

If the entire network is connected to the Internet, it can be easily breached, unlike in the case of Stuxnet, which had an Air gap, which made it difficult to put the payload in the network, which was then delivered using infected USB.[3]

Assuming that there is a ransomware attack(encrypting and locking data), there are other facilities for storing these data in physical form at the distributed locations, getting inspired by duqu, flame and gauss-like malware attacks.[3] Here we are looking at a more serious issue of controlling physical components using this attack, just like Stuxnet did. Most components like boilers, combustion chambers and some more dangerous equipment are directly controlled using computerised systems, so increasing temperature above the critical temperature can cause an explosion to the entire gas power plant.[4]

Chapter 3

Cyber Detterence Challenge

The attackers might have built payloads to be very stealthier that have a self-killing task, just like in the case of duqu. After thirty-six The malware would delete itself entirely from the system after operating on a target. This feature made detecting and analyzing Duqu incredibly difficult for security researchers – forensics.[5]

The difficulty of finding the attackers as they might be hiding their locations or misdirecting us to some other people. If they are misdirecting us to other people by providing us with the person's private data, then it will be legally wrong to work in that direction.[6]

If we are under attack and the entire system and network are infected, it would be impossible to predict whether the attackers are trying to steal the data, encrypt the data(ransomware), or attack the power's physical components.[6]

Further, if there are no prominent signs of damage or reduced performance after the system is infected, then it can be challenging to find whether the system is infected or not, and the malware can easily self-propagate to more systems in the network, stealing more data or trying to launch a more severe attack at some prominent time. There can be considerable potential for damage due to counter-retaliation

Chapter 4

Legal and Treaty Assumptions

Points that can be included in the treaty with Hostile Nations:

1. Countries should not knowingly allow their territory to be used internationally wrongful in the domain of cyberspace.[7]

2. A country should not conduct or knowingly support cyber-criminal activity. Contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to another country's public.[7]

3. Countries should not conduct or knowingly support activity to harm the information systems of another country's authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams).[7]

Points that can be included in the treaty with Friendly Nations:

1. Countries should consider how best to cooperate in exchanging information, assisting each other, prosecuting terrorists and criminals involved in cyber threats, and implementing cooperative measures to address such threats. Countries may need to consider whether new measures must be developed in this respect.[7

Points that can be included in the treaty with Friendly Nations:

1. Countries should encourage responsible reporting of vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.[7]

Common points to be included in treaties with all nations:

1. **Building Confidence and Trust**: The identification of appropriate Points of Contact (PoCs) in the policy and technical levels can facilitate secure and direct communications between countries to help prevent and address severe incidents and de-escalate tensions in crises. Communication between PoCs can help reduce tensions and prevent misunderstandings and misperceptions that may stem from cybercriminal incidents, including those affecting critical infrastructure with a national, regional or global impact. They can also increase information sharing and enable countries to manage and resolve cyber-attacks more effectively.[7]

2. **Providing Transparency**: Exercising Transparency voluntarily through the exchange of national views and practices on cyber security incidents and other related threats and by making cyber security advice, guidance, evidence base and data supporting decisions publicly available is essential for building trust and predictability, reducing the possibility of misinterpretation and escalation, and helping organizations and agencies make good risk management decisions.[7]

Chapter 5

Solution Architecture

The Air Gap in the Natanz nuclear enrichment facility made the task for the attackers somewhat difficult. Connecting the internal network of the Gas Power Plant with the external network like Internet can give attackers one of the ways to introduce the payload into the system. With an air gap in place, the attackers would need to physically introduce the payload using infected CDs, USBs, or any other infected external device.[3]

The next step is protection from the infected external device. Using Antiviruses and extensive measures like Intrusion Detection Systems(IDSs) to protect the system from external devices.[8]

The most important thing is securing CPS. Cyber-Physical Systems (CPS) are designated as essential components of the Industrial Internet of Things (IIoT), and they are supposed to play a key role in Industry v4.0. CPS enables smart applications and services to operate accurately and in real-time. A CPS is identified as a network of embedded systems that interact with physical input and output. In other words, CPS consists of the combination of various interconnected systems with the ability to monitor and manipulate real IoT-related objects and processes. Despite their numerous advantages, CPS systems are prone to various cyber and/or physical security threats, attacks and challenges. This is due to their heterogeneous nature, their reliance on private and sensitive data, and their large-scale deployment.[8]

To prevent any targeted attack on the physical parts of the gas power plant using the CPS system, we mainly need to protect CPS from being compromised.

Exploring the architecture and working of the CPS System

CPS layers

The CPS architecture consists of three main layers, the perception layer, transmission layer, and application layer.

Perception Layer: It is also known as either the recognition or the sensing layer. The power plant includes equipment such as sensors, actuators, aggregators, reactor parameter monitoring systems, along with various other devices which come under this layer. These devices collect real-time data in order to monitor, track and interpret the production in the plant.

Transmission Layer: It is also known as the transport layer or network layer, and it is the second CPS layer. This layer interchanges and processes data between the perception and application layers. Data transmission and interaction are achieved through the Local Area Networks.

Application Layer: It is the third and most interactive layer. It processes the received information from the data transmission layer and issues commands, which are executed by the physical units, including sensors and actuators. This is done by implementing complex decision-making algorithms based on aggregated data. Moreover, this layer receives and processes information from the perception layer before determining the rightly invoked automated actions.[8]

Protecting Data in the application layer can be done using anonymization, data masking, privacy-preserving and secret sharing.[8]

These layers can be easily broken into some main components like SCADA (supervisory control and data acquisition), DCS (distributed control system), and PLC (program logic controller). The main role of SCADA is to gather and control geographically dispersed assets ranging from controlling sensors within a plant to controlling power dissemination in a country. DCS, on the other hand, controls the controllers

that are grouped together to carry out a specific task within the same geographically location. Both SCADA and DCS use PLC devices to control the industrial components and processes.[9]

Cyber Attacks can compromise the communication between the application layer and transmission layer by targeting the control system by compromising workstations used to reconfigure the Programmable Logic Controllers (PLCs) for facility operations and tampering with messages sent from the system operator to the PLC. Just like Stuxnet modifies control messages in order to increase the frequency of nuclear centrifuges to unsafe levels, leading to equipment failure. So, control messages need to be secured in order to ensure the authentication of the source, detect modification of received messages and prevent the attack. Securing communication between the operator and PLC can be achieved by either using the same cryptographic key for all messages or using a different key for each message. The American Gas Association (AGA) presented its AGA-12 standard to provide "bump-in-the-wire" encryption services for CPS. Similarly, we can also implement such cryptographical encryption services to secure the communication between the layers. Further, we can use the Shadow Security Unit(SSU) introduced by TAIGA(Trustworthy Autonomic Interface Guardian Architecture), which is complementary to the existing SIEM architectures, and it can transparently intercept its communication control channels along with its physical process Input/Output lines to constantly assess both security and operational status of PLC.[8]

Apart from this, CPS behaviour can be predicted through the implementation and use of artificial intelligence or/and even Machine Learning (ML) schemes. This allows the prediction of the so-called "next-time system state". If the behaviour differs from the predicted behaviour, we can check for any infection if present using some CPS testing tool like Achilles.[8]

Now, as in the case of Stuxnet, the payload infected many systems in the facility using the vulnerability present in the windows operating system. For this, we need

to keep the software always updated so as to patch up the possible vulnerabilities that can be present in the older versions. We can also use firewalls and deception techniques like Honeypots.

Furthermore, there is a need to have a manual intervention that can be used in emergency situations independent of all CPS systems.

Chapter 6

Benchmark for success

Q1. What does success look like when trying to prevent a cyber warfare attack on a critical infrastructure?

Ans: While preventing a cyber attack on critical infrastructure, success will mean:

1. The attacker could not gain access to the data of the infrastructure.
2. There is no damage to the physical components associated with the infrastructure.
3. The point from which the payload needed to be penetrated worked perfectly to prevent the attack at an early stage.

Q2. What does success look like when under a cyber warfare attack?

Ans: When under a cyber attack on critical infrastructure, success will mean:

1. Preventing the attacker from taking control of the entire system.
2. Restricting the self-replicating nature of the malware/attack.
3. After the attack is nullified, collecting the points that can lead us to identify the attackers.

Q3. What does success look like when asked to launch an offensive?

Ans: When launching a offence against the cyber attack, success will mean:

1. No damage was caused to the system due to any counter-retaliation.

2. Collect all the data about the attackers so that analysis like forensics can connect the dots to find most information about the attacker.

Chapter 7

References

1. Power Plant Automation: Where We Are and Where We're Headed
2. NTPC gas power plant Auraiya, Uttar Pradesh
3. The History of Stuxnet
4. Open Cycle Gas Turbine
5. After Stuxnet Acknowledging the Cyber Threat to Nuclear Facilities
6. Attack Analysis
7. Legal and Treaty Assumptions
8. Cyber-physical systems security: Limitations, issues and future trends
9. Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet