Cybersecurity in Power Grids

1.Methodology and Assumption-:

1.1 Abstract

Modern power grid control systems are not isolated islands, as a failure in one system might result in instabilities or even blackouts in other systems. Cyber-attacks on power grids have the potential to cause enormous financial damage. Indeed, cyber-attacks on power systems have recently succeeded in creating large-scale, temporary blackouts. For example-:

1. The European Network of Transmission System Operators for Electricity (ENTSO-E) which represent 42 European transmission system operators in 35 countries, was successfully hacked in 2020.

2.In June 2019 Russia becomes the target of US launched cyberattack.

3.In December 2015 hackers got into the system of Ukrainian Power company cutting power to 225,000 household.

4. Also China was suspected to be behind the power outage in Maharashtra.

In this research paper, we first take broad overview on the inner working of power grid that emphasizes the identification of key elements of the infrastructure, further we analyse the infrastructure of power grids to derive resulting fundamental challenges of power grids with respect to cybersecurity which in turn help to point out the main source of vulnerabilities. Moving further we define a solution architecture along with its benchmarking and its connection with rest of the world. Moreover, the approach can be adjusted to develop security systems for other critical infrastructure assets such as gas and chemical processing facilities, water, and wastewater systems.

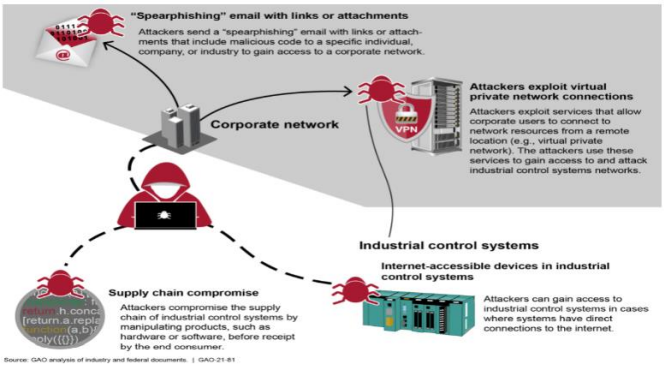

Fig-1: Showing various type of attack possible by an attacker.

1.2 Introduction

Every country's key infrastructure, particularly the power grid control system, is critical to its economy. Cyber-attacks on power grid control systems might have a huge impact on entire countries or even continents. Therefore, designing and implementing

cybersecurity measures for power grid control systems is critical and can only be examined from the scratch.

1.2.1 Basic structure:

An electrical grid is an interconnected network for electricity delivery from producers to consumers. Electrical grids vary in size and can cover whole countries or continents. It consists of following key components-:

- Generation-: The process of generating electric power from primary natural resource.
- Transmission-: The bulk movement of electric energy from generating site to consumption site. One of the major security challenging level.
- Substation-: Part of electrical generation, transmission, distribution system whose main function is to transform voltage i.e., step up or step down.
- Distribution-: The final stage in the delivery of power, it carries electricity from the transmission system to individual consumers. One of the major security challenging level.

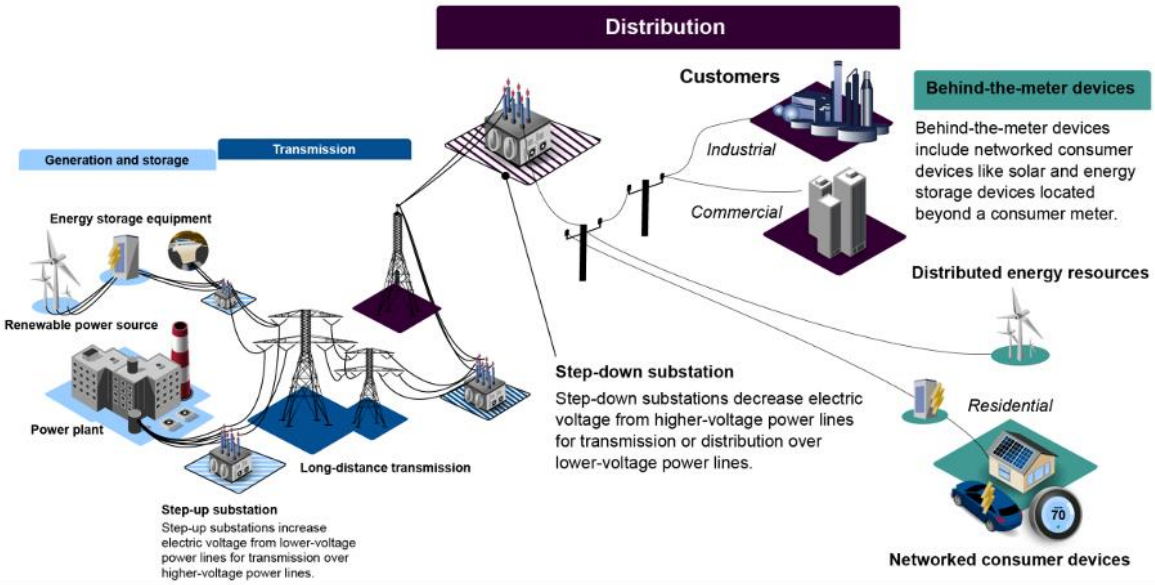

Fig-2: Showing various key component involved in power grid

1.2.2 Power grid system analysis

Due to increase in the need of more power resource involved in various domains we have two choices 1st: Is to plant more generation plants; 2nd: To increase efficiency of power grid. And as we know due to less availability of land resource it is wise to move on to considering 2nd choice. And this step is now feasible with advancement in technology and digitalization of power grid, which in turn increases connection with larger communication networks (server/internet), resulting in large number of dataflows, which constitute critical infrastructure and raises severe security concerns.

Protocols and systems originally developed for power grids were not designed with security in mind. Yet, these systems are still used alongside modern technology and increasingly exposed to outside networks, such as the Internet. Likewise, the increasing use of digital and decentralized technology provides a larger attack surface. Indeed, different cyber-attacks have successfully targeted essential parts of the power grid. Resulting disruptions and wide-scale outages of electrical power have extensive social and economic consequences.

1.2.3 Communication infrastructure of Power grid-:

Due to change in amounts and means of communication, which is necessary, more and more communication channels are established which in turns increase the vulnerabilities. Transmission of power is overseen by transmission system operators (TSO), while the distribution of power is carried out by distribution system operators (DSO).

Typical to the network of a grid operator is the separation between office network and process control network (PCN).

- Office network-: It is like any usual corporate network with, e.g., email traffic or data processing
- PCN -: the PCN connects the control room of grid operation companies with their substations and field devices, typically using DNP3 (North America and parts of Asia) or IEC 60870-5-104 (rest of the world) as protocol.

  Resulting control messages are usually interpreted by a programmable logic controller (PLC) and then passed to the process layer. The control room typically contains a human-machine interface (HMI), a database (DB) server managing grid information, and a simulation server for pre-computing the effects of grid changes. Furthermore, the control room is connected to multiple substations (each containing at least a gateway, an HMI, and multiple PLCs) and can be coupled with other TSO/DSO SCADA systems for mutual control.

  Data exchange between office network and PCN should only be handled through a dedicated data exchange server, where every file is checked for malware before being passed through. Sometimes, though, as seen in the Ukraine attacks, there are other communication channels, such as VPNs, which allow direct communication between the office network and the PCN or remote maintenance lines for vendors or contractors.

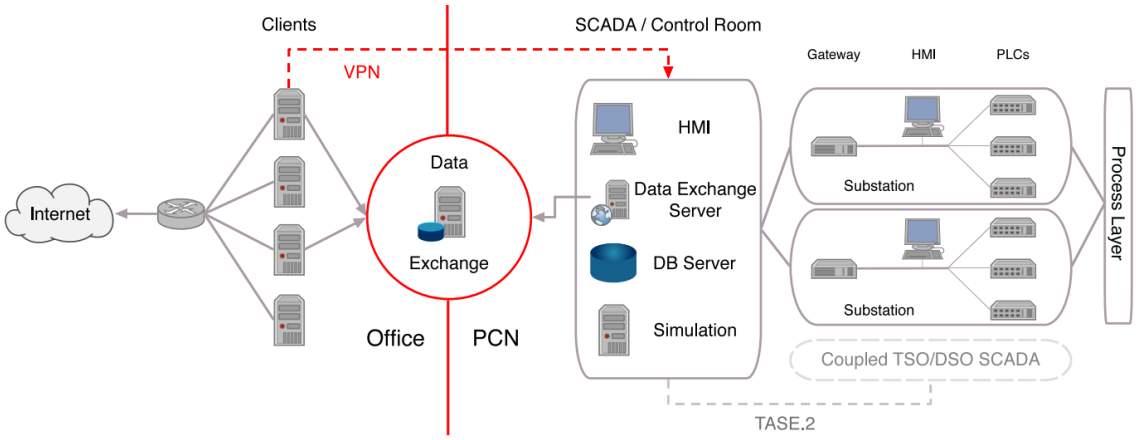

Fig-3: showing communication infrastructure of power grid

1.3 Methodology

The methodology that the malware is assumed to use here in this research paper is inspired from past incidences and the key vulnerabilities that are easy to target.

Examples of past incidences which involved here are -:

- BlackEnergy -: shut down Ukraine power grid in Dec 2015.
- CrashOverRide -: Again, Ukraine in 2016
- Sandworm -: Against NATO.

At first hacker uses variety of vectors so as to gain access to victim's network, including mails, watering hole attacks, Trojanized software or USB insertion, which further leads to spread infection either to an organisation or global.

Malware uses the idea of mapping internal IT network of a transformer station and sabotage it. It attacks SCADA system, which monitors and controls a full set of industrial equipment. Traditional method of transmission involves use of copper cable but after optical fibre came into picture system becomes more vulnerable to attack. It opened a backdoor that allowed the attackers to control infected machines to a level where they were able to cross over into the operational network. Once there, they started to flip switches, disabling IT infrastructure and deleting files.

CrashOverRide virus is flexible enough to automate and manage large-scale power disruptions. It has the ability to control the switches and circuit breakers of older energy substations, allowing an attacker to simply turn off power distribution, triggering cascading failures and more serious equipment damage.

1.4 Assumptions

1. In this report our prime focus is on the communication, transmission, and distribution of power through power grid.
2. Ideally it is considered that cyber-attack must be perform by the foreign person/organisation/nation, which is not related to organisation, else if it is insider

then he must have access to much information prior and it makes no point in figuring out this case, as this case can be treated as individual question. For ex-: Leave the case which happen in Australia regarding sewage problem.

3. Data exchange between office network and PCN should only be handled through a dedicated data exchange server, where every file is checked for malware before being passed through.

2. Solution Architecture

As the Power grid system involves multi-level authentication system so, I frame the architecture like that of SCADA systems. The architecture which I present in the following section is the extension of OSI and PRM models. So before moving on first let us recap a little bit about this architecture which also helps us to find out the challenges involved in this type of architecture.

2.1 Layer Architecture

The architecture design pattern in which the whole network or design is divided into small parts, and each small part is assigned a different layer with appropriate authentication system and functionality.

This type of design pattern is used when-:

- Building new facilities on top of existing system.
- When development is shared across several teams with each team assigned a particular layer to work upon.
- When there is requirement for multi-level security.

Advantages-:

- Allow replacement of layer without disturbing the whole system.
- Authentication system can be provided in each layer.

2.2 Protection system requirements

To identify the cybersecurity protection of a system, the following top-level objectives with regard to the technological infrastructure should be considered:

- Creation of dedicated protection mechanisms that ensure an adequate level of cybersecurity against cyber-crime.
- Continuous monitoring of cyber threats in the IP network infrastructure that supports power generation control and management subsystems.

Traditional information technology protection solutions cannot be applied directly to control systems due to their tight real-time operational limits as the power grid becomes more digitalized and technology advances. In other circumstances, new customised security solutions are required because typical security measures may not be sufficient to ensure the safe operation of industrial control systems because security is not their

primary concern. Furthermore, the cost of potential harm in the case of power grid control systems is just too expensive.

2.3 Design and Implementation

According to Layer architecture, Power grid must be divided into layers to form layer type structure. So, we divide the Power grid layer on the basis of functionality that a particular layer performs. Thus, it can be divided into 3 major layers-:

1. Physical system -: comprises of Physical layer and control layer.
2. Cyberspace-: consist of communication and network layer
3. Application layer-: consist of management and supervisor layer.

Each layer can be further divided into 2 sublayers to form in total 6 layers as-: physical layer, control layer, data communication layer, network layer, supervisory layer and management layer.

Let us focus on each layer individually-:

1. Physical layer-: This layer comprises of the physical plant to be controlled. It is often described by model-free statistics.

   Because grid operators frequently communicate over their own physical networks, physical security is inextricably linked to cybersecurity. A determined attacker may, for example, get into a substation and infect local equipment with malware or otherwise meddle with PCN access.

   Physical security for substations varies greatly among grid operators but can be as simple as a wire fence with no surveillance or access control. Protection of substation information, such as engineering drawings and power flow models, as well as surveillance and monitoring methods, such as video cameras and motion detectors, as well as physical access restrictions, are all recommended steps to provide physical security for substations.

   Physical security that is more advanced may not only discourage intruders but also serve as part of a broader IDS. For example, if a substation has a physical security violation, subsequent hostile activity in the PCN could be linked to the physical security violation, aiding in attack response. Integrating (automatically) identified physical security infractions into an overall security solution comprising IDS on the network side would be a key problem. The difficulty of physical security is being magnified as new, easily accessible assets, such as smart metres and charging facilities for electric vehicles, are being integrated into the communication backbone of smart grids.

2. Control layer-: It is controlling layer which consist of multiple control components like sensors, IDSs, actuators, firewall etc. whose main function is to estimate the state of current system with the help of sensors, which collects the data from physical layer. Sensor data can be fused locally or at the supervisor level for global fusion.

   IDSs and firewalls are used to protect the physical layer. IDSs perform the job by monitoring network traffic for any suspicious activity and issue alerts to supervisor when any such activity occurs. An anomaly-based ID is more

common for physical layer whereas signature based ID is more common for packets or traffic at the communication layer. There lies a fundamental trade-off between local decision vs centralized decision. A local decision, for example, made by a prevention system, can react in time to unanticipated events; however, it may incur a high packet drop rate if the local decision suffers high false negative rates due to incomplete information.

3. Communication layer-: This layer acts like an intermediator between different layer as it handles communication which involves communication between different layer or devices via communication cables. This layer primarily involved in connection between control layer and network layer routers. The communication channels can be of the form of physical cables or wireless.
   As we discussed in previous sections this layer is most vulnerable to cyber-attacks and privacy issues and thus should be primarily protected. Communicated messages and keys should be encrypted before transferring to destination as this type of layer is most vulnerable to man-in-middle attack. Also, important messages and things should also be backed up in some sort of alternate database as it can heavily face DOS attack like that of Sony company and if such a situation arise there is no means of recovering it.

4. Network layer-: This layer works upon the principle of making randomize routes or path which leads to a certain minimum delay by an attacker. Even though it does not completely remove the chance of an attack but then also provide enough number of time and energy so as to minimize the attack situation or demands enough number of resources for a successful attack.
   It comprises of mainly two components-: 1. Network formation, 2. Routing. In case of routing, we form a number of randomize routes to disguise the attacker.

5. Supervisory layer-: This layer serves as the system's brain. It designs and sends necessary commands to all layers in order to coordinate them. Its primary purpose is to undertake essential data analysis or fusion in order to provide an accurate and timely assessment of the situation. It's also a comprehensive policymaker who efficiently distributes resources. Communication resources, maintenance budgets, and control efforts are all included in the resources.

6. Management layer-: The management layer is a higher-level decision-making engine that approaches resource allocation challenges in control systems from an economic perspective. At this layer, we address issues such as (i) allocating resources to various systems in order to achieve a goal; and (ii) patch management for control systems, e.g., disclosure of vulnerabilities to vendors, development and release of patches.

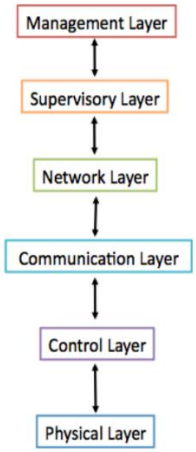

Fig-4: Showing layer architecture of power grid.

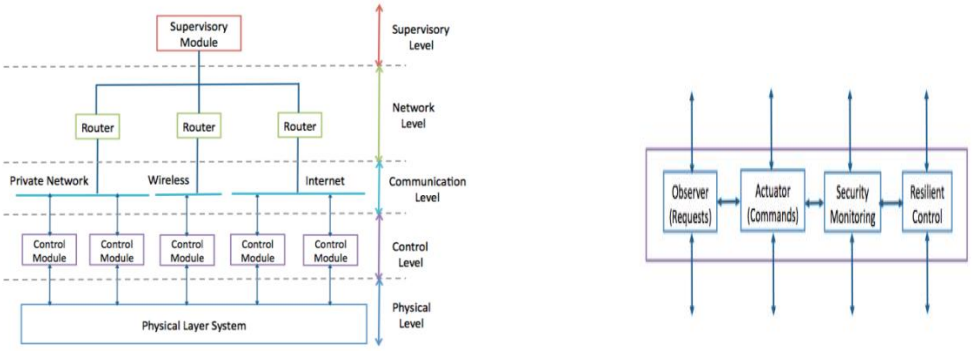

Fig-5: showing actual architecture design and its implementation.

3. Cyber Deterrence Challenges

3.1 Existing challenges in current architecture-:

1. CIA triad-: it stands for confidentiality, integrity, and availability. In general literature of cybersecurity trends, confidentiality and integrity are prime important elements to be considered and can sacrifice availability. But in power grid analysis availability is most important as its consequence of downtime is severe. And thus, any measures ensuring confidentiality and integrity should not interfere with availability, which in turn decreases Confidentiality and Integrity of system.

2. Balance between Generation and Consumption-: Power grids rely on a 50-60Hz steady frequency. Because power generation and consumption in the operational reserve include temporal delays, attackers target this stable equilibrium because they only need to manage a very small quantity of consumption or generation to utilise cascading effects inside the grid to generate a system-wide blackout.
3. No security in PCNs-: Many power grids still utilise classic PLCs that were created decades ago and lack security since security was not a priority at the

time. These PLCs and protocols are a key source of vulnerability in today's big cyber-attacks.

3.2. Challenges related to Solution architecture

1. Performance degradation due to multiple level of a service request as it is processed in each layer.
2. Control layer has a major concern on whether the diagnosis and control modules need to operate locally with IDS or globally with supervisor.
3. Due to separate layer for communication, it becomes easier and clearer for attacker to target to one portion of layer to get access to most of the credentials and information of the system.
4. It is essentials for the engineers to build the physical system with more dependable components and more reliable architecture. And this brings concern on the physical maintenance of control system that demands cross layer decision making between management and physical layers.

3.3. Other challenges

1. Till date it is very cumbersome and difficult task to identify the source and origin of attack as technology is improving daily and many means are there to hide the deeds.
2. Like in solution architecture I had talked about creating various randomize routes so as to disguise attacker in the same way attacker can also misguide ourselves to point all committed things to other parties.

4. Legal and Treaty Assumption

It refers to a legally binding arrangement, such as a contract, which establishes obligations between two or more international law subjects. In this research paper we define laws and actions which I suggest to be taken in the case of cyberattack by a nation.

Common Actions in all three scenarios-:

a. The state should first hold a joint conference along with the suspected attacker nation so as to discuss each party’s view on the topic, and give evidence against the nation, and nations itself gives evidence in favour of it so as to protect it, as we know there are quite techniques so as to disguise research team.

b. If found guilty specific action must be taken which are already defined in the constitution or law book of the victim's country.
c. On the basis of severity of attack one can also raise trade barriers or could limit trading with that country.

1. Friendly nation-:
    a. Prior to any action we can also suggest PMO to hold personal meetings of Prime ministers and/or President meeting of respective states.
    b. One should now keep an eye on the activities of the nation as it is no more much trustful as before, i.e., It decrease its status level of being friend.

2. Neutral nation-:
    a. On the basis of severity, it has decreased to level of somewhat closer to hostile state, so we must have to keep close look into the activities of that nation.

3. Hostile nation
    a. Strict laws should be made against them.
    b. Keep a strong watch on the activities of them and cyber forensic team should be made so as to keep analysing all their movements.

5. Benchmarks for Success

It refers to measure of an organization's baseline of security/action against competitors and standards so as to improve it further. It is one of the key components to mention as cyber threats are constantly evolving and the processes and technology needed to prevent them are constantly changing. So, we need to have measures in place to frequently assess the effectiveness of the safeguards you have invested in. Key performance indicator (KPI's) is important method so as to analyse the cybersecurity theme that is currently in use.

Success can be looked in three major scenarios-:

5.1. Parameter to measure success when trying to prevent cyber warfare attack:

a. Preparedness level-: When number of devices in corporate network to become fully patched are less, i.e., most of them are up to date.
b. Intrusion Attempts-: When many number of times our suggested architecture is able to prevent unauthorized access.
c. Patching Cadence-: Attacker mainly target in the time gap between patch release and implementation. So, success is felt if time lag is less and more importantly no such attack could happen during that period.
d. Vendor Patching Cadence-: When most of the critical vulnerabilities are removed from third party vendor.

5.2. Parameter to measure success when under cyber warfare attack-:

a. Security incidents-: When number of times an attacker had breached our system information is less and also minimum quantity of information is stolen.
b. Mean Time to Detect (MTTD)-: It refers to mean time for which threat go unnoticed. So, success is seems to be met if MTTD is significantly less and no such major issue happened during that period.
c. Mean Time to Resolve (MTTR)-: It refers to mean response time for a team to respond to cyber-attack. Success is felt only when MTTR is less, and proper measure had been taken down.
d. Mean Time to Contain (MTTC)-: It refers to mean time for a team to identify all attack vectors across all endpoints. It is also should be less for success to be felt and no major harm had been happened to any device and equipment.

5.3. Parameter to measure success when launching an offensive attack-:

a. Downtime-: When the system and server of the targeted organization is down for large period of time and employees are not able to do contact or do work.
b. Number of incidents by category-: When large and diverse amount of successful attack happened, and organization is unable to prevent it.
c. Mean Time to Detect (MTTD)-: When MTTD is quite large and in that period, malware keep performing its assigned task like in the case of Stuxnet.
d. Unidentified end point vectors-: when targeted organization is not able to identify all vectors present in end points and thus not able to patch up all the vulnerabilities which leads to excess of entry points for attackers.

6. Prototype

I have made following code which are useful for initial phase of attacks and also I have tried to make a small malware whose function is to corrupt all .py extension files in directory and print an infinite loop and also store data, i.e., code in a list.

GitHub Link-: https://github.com/Yashgupta03/cyber_security

Actually, Attack or Defence folder contain file related to these approaches only whereas dummy_malware contains malware and ransomware which I had made while studying during the course.

Attack and defence are taken from lecture, whereas malware is implemented by me.

7. Conclusion

Technology is evolving daily and so the threat is also becoming prevalent because of which cyber security becomes very important to consider. Due to digitalization and

modernization need for more efficient power grid is prime important, but because of this communication also becomes more which result in serious vulnerabilities. And to prevent our system best against it need for better architecture is required.

In this paper we have looked for possible design of malware which we predicted from key vulnerabilities and past incidences and, looked for a better architecture so as to prevent this type of malware if detected, also I suggest some key points which we can look so as to actually define success and benchmark it for same.

8. References

1. Krause, T., Ernst, R., Klaer, B., Hacker, I. and Henze, M., 2021. Cybersecurity in power grids: Challenges and opportunities. *Sensors*, *21*(18), p.6225.
2. Zhu, Q. and Basar, T., 2012. 17 A hierarchical security architecture for smart grid.
3. Jarmakiewicz, J., Parobczak, K. and Maślanka, K., 2017. Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection*, *18*, pp.20-33.