Cyber Security challenges in Electrical power Infrastructures: India's Perspective.

Abrar Ahmad*, Md. Sajjad Ahmad

**Assistant Professor – Jamia Millia Islamia, Research Scholar – Jamia Millia Islamia*

aahmad15@jmi.ac.in

Abstract

This paper explores various cyber security concerns from India's perspective. With rising data communication among devices and cloud based information for fast and dynamic response, the multitude and magnitude of cyber vulnerability against attacks are also aggravating. India which happens to be a strategic nation with various geopolitical foes and friends, the propensity of cyber attack against India's power system cannot be discounted. This paper explores the potential modus operandi of cyber attack on power infrastructure and outlines possible defence mechanism to suppress such events. The paper also discusses Ukrainian Grid attack and lesson that can be incorporated for such eventuality in case of India and beyond.

Keywords: Cyber security, Power Grid, Cyber-attack, Smart Grid.

Introduction

With ever increasing power system management tools integrated with communication network, and centralization of power management, the chances of cyber-attack is at higher risk especially after convergence of IEDs, IoTs, Internet based SCADA, and smart grid implementation. It is understood that with the advent of 5G communication technology and seamless sharing of information, the concern for cyber security will pose even greater threats. India has been a target of cyber-attacks, with 529 federal and state government websites being hacked since 2016 [1]. Indian power system is 3rd largest power producer and consumer in the world with 371 GW of installed power and 36% penetration of renewable energy, India's per capita consumption of power stands around 1181 kWh [2] A cyber-attack can put a nuclear power plant under very high risk if its enrichments of fuel malfunction. Similarly slew gates of hydropower plants can not only affect the performance of power generation but may also endanger lives of people at the lower side of flood plains.

On December 2015, quarter of million people lost power in Kiev, the Capital of Ukraine. It was suspected that foreign Hackers send emails to power officials, and installed malware to effectively control a section of Ukrainian power system. Seven 110 kV and twenty three 35 kV substations were disconnected for three hours [2]. Later statements indicated that the cyber-attack impacted additional portions of the distribution grid and forced operators to switch to manual mode. Shortly after the attack, Ukrainian government officials claimed the outages were caused by a cyber-attack, and that Russian security services were responsible for the incidents [3]. Similarly a series of power outages in Los Angeles, San Francisco, and New York City left commuters stranded on 21.04.2017, yet to be recognized, whether due to cyber-attack or a malfunction [3]. In India, Some high profile cyber-attacks includes the November 2017 malware attack on THDC Ltd.'s Tehri dam in Uttarakhand, the May 2017 ransom ware attack on West Bengal State Electricity Distribution Co. Ltd (WBSEDCL), the February 2018 attack on a Rajasthan discos website, and the March 2018 attack on Haryana discos in which the commercial billing software of the highest paying industrial customers was hacked [4]. About 52% of domestic companies said they fell victim to a cyber-attack in the last 12 months despite having independent security budgets, according to a Sophos survey The Future of Cyber security in Asia Pacific and Japan [5]

Cyber Security and Cyber-Attack

The protection of equipments, communication network, architecture (hardware and software) of any automated system for attack, damage or improper function is called Cyber security. Any breach to this security can be either random or intentional. If the damage to cyber security is intentional it would termed as Cyber-Attack. Cyber security assesses and identifies potential networks and systems vulnerable to attack and implement infrastructure to ensure security.

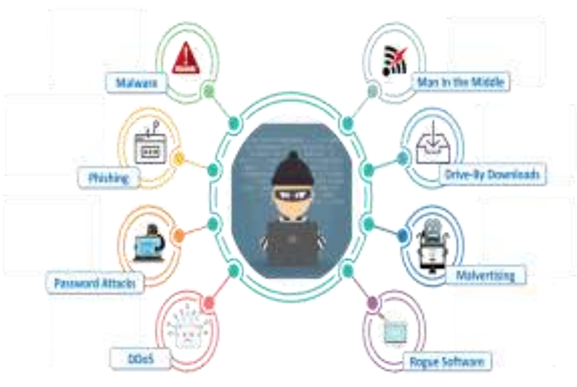

Figure 1: A schematic of various cyber attack potential

Following pie-chart as shown in Figure 2 is showing the result of cyber-attacks on different infrastructure in United States. It is very clear from the chart that energy sector is most vulnerable sector for cyber-attack followed by critical manufacturing and communication infrastructure. 79 incidents have been reported in the year 2014 as provided by US homeland security department [3].

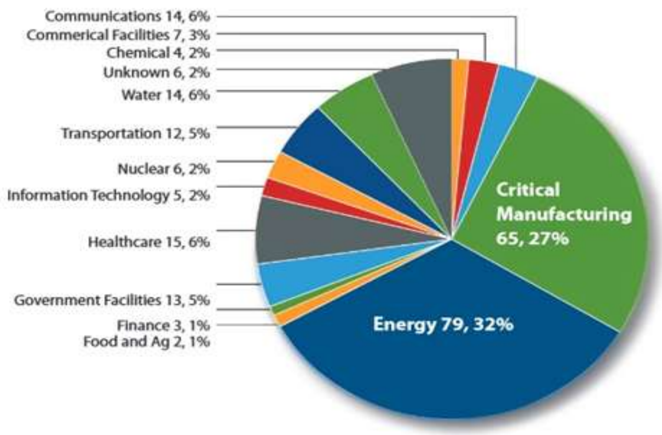

Figure 2: Cyber-attack share in different industries

Modelling a Modus Operandi of Cyber Attack in Power Systems

The two main steps of any cyber-attack are intrusion into the intended facility and disturb or disrupt the proper functioning of a power system or in other words attack. The Cyber-attack starts with intruding into credentials of the power infrastructure. The attack could be random closing an opening of circuit breakers thereby disturbing power line topology or specific action aimed at blackout of the regional or national grid. In the past it has been manifested that the attackers had the capability to gain a foothold and harvest credentials and information to gain access to the power system information network. Additionally, the attackers can also operate through supervisory control system; such as the Human Machine Interface (HMI) as explained in figure 3.

As mentioned in above figures, reconnaissance or planning of the intended target is first stage for potential cyber-attack. Interesting targets are those where high level of automation in the distribution system is present; enabling the remote opening of breakers in a number of substations. While the initial footholds were used to harvest legitimate credentials for pivoting and systematic takeover of IT systems and remote connections, it is likely that the attackers move quickly away from their initial footholds and blend into the target's systems as authorized users. With this information, the attackers would be able to identify VPN connections and avenues from the business network into the ICS network. Using native connections and commands allows the attackers to discover the remainder of the systems and extract data necessary to formulate a plan for attack.

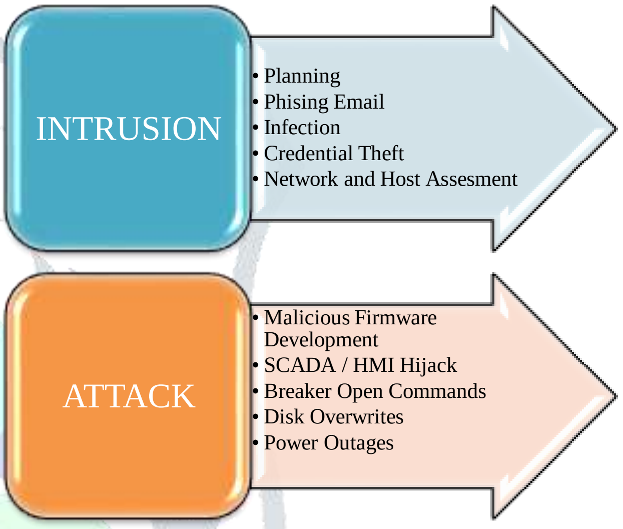

Figure 3: Intrusion and Attack in power system

The adversary may conduct follow-on attacks that pursue alternative forms of social engineering campaigns, like targeting the organization through large-scale phishing campaigns, using water-holing attacks, or conducting direct-call campaigns to users or the help desk.

There are three types of attacks that can happen during a cyber-attack on power system infrastructure

1. Supporting attack (not effective individually)
2. Primary Attack
3. Boost Attacks

The peripheral attacks as the name suggest are not to do with core functioning of system but rather attacking the supporting infrastructure like switching of power supply or shutting the access to server etc. It could also disconnect the communication between system and consumers thus affecting the overall reliability of the infrastructure. These attacks however don't affect much and less prone and the attacker don't achieve much by this method. Primary attack is the actual cyber-attack where vital infrastructures are hijacked and attackers are able to manipulate the functioning of relays, circuit breakers, transmission networks and substations to push the power grid into a manufactured blackout.

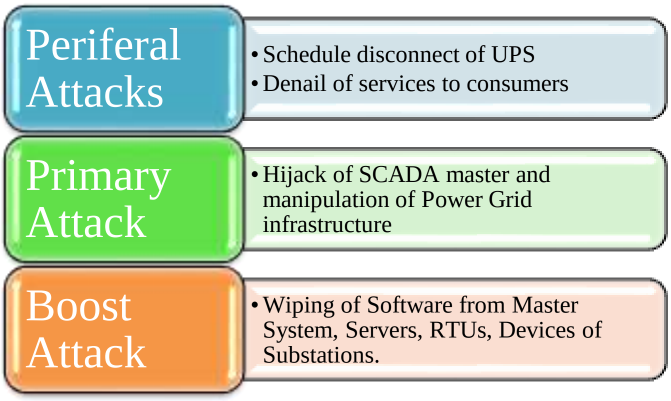
Periferal Attacks
• Schedule disconnect of UPS
• Denail of services to consumers
Primary Attack
• Hijack of SCADA master and manipulation of Power Grid infrastructure
Boost Attack
• Wiping of Software from Master System, Servers, RTUs, Devices of Substations.

Figure 4: Stages of Cyber-Attack.

The attackers may first learn how to interact with the three distinct DMS environments using the native control present in the system and operator screens. Also they may develop malicious firmware for the serial to Ethernet devices network connected to a UPS in order to reconfigure it so that when the attacker caused a power outage, it was followed by an event that would also impact the power in the energy company's buildings or data centres/closets. In boost attack the attackers could intend to delay the restoration procedures thereby deleting software from master system, bugging the server and other soft infrastructures. This is why architecture of the system should be framed to have backup arrangements in order to restore the system as soon as possible.

Cyber Security Challenges in India

Indian power sector is in developmental stage with lot of private players are foraying in its GENCOs, TRANSCOs, and DISCOs; all of which equally susceptible for cyber-attack. The electricity market with more and more power exchanges such as IEX, PEIL etc. are coming with more and more power transaction routes based on power supply and demand between different players. More the number of nodes, the more are potential for cyber-attack potential intrusion points. The rising of renewable energy penetration to the power system is also a cause of concern from cyber-attack point of view. This increases the need for fluctuation and power flow which demands more real time information thus enabling more hot-spots for information phishing. The Increasing grid complexity with more and more nodes and bodies for power handing and seamless power transfer from north to south and east to west increases the nodes and information sharing.

Another cause of concern is increasing need of automated controls. Although the control systems have been using open protocol for better control market but this raises vulnerability from security angle. The rising capability of such equipments is also a concern as the more the capable higher the impact of its malfunction. Mostly, the power infrastructure of India are designed for better reliability and safety as cyber-security is relatively new challenge, therefore old infrastructure may not have accounted for cyber security concerns. Foreign Players in privatized electricity market sometime can also lead to relative vulnerability. For example, Australian Government in 2012 had intervened to block a privately owned Chinese Communication Company from winning lucrative contracts to help build the $ 36 billion fibre optic National Broadband Network. The decision, it seems was based on the advice from the Australian Security Intelligence Organization (ASIO).

The danger also lies in supply chain of electrical utility products as depicted in Figure 5. The critical network equipment and special cyber security products can only be sold or provided after being certified by a qualified establishment, and are incompliance with national standards.

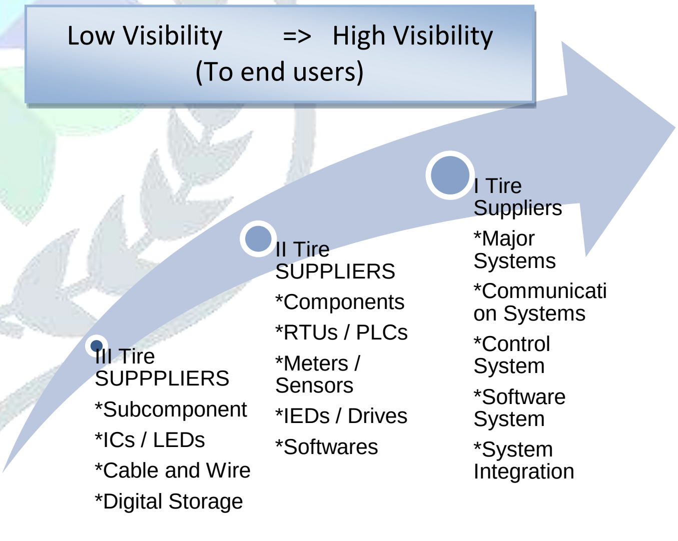

Figure 5: Schematic showing vulnerability of utility equipments

Defending a Cyber-Attack

As a defender to cyber-security one need to develop anticipatory response system to nullify attack effects. The automatic system need to be clearly reviewed from cyber-attack perspective and any communication with doubtful areas should be segmented, monitored, and controlled diligently. Each email coming into the network should be using proxy systems to control outbound and inbound communication paths, thus limiting system infrastructure to communicate only through the proxy devices by implementing perimeter access controls. User account behaviour should be monitored along with network and system communications at directory-level. Any abnormalities must be identified and should be alarmed to the cyber defenders. Implement alarm capabilities with different priority-level alarms based on the risk of the systems associated with the alarms. Decision makers should review their restoration plans for attacks with the potential to go deeper into the ICS and could result in damaged equipment.

The defence system can be categorized as planning at Architecture level, development of passive defence mechanism, deployment of an active defence system, collection of intelligence and legal countermeasure to confront adversaries and diminish any further chances of cyber-attack. The same is elaborated in figure 6.

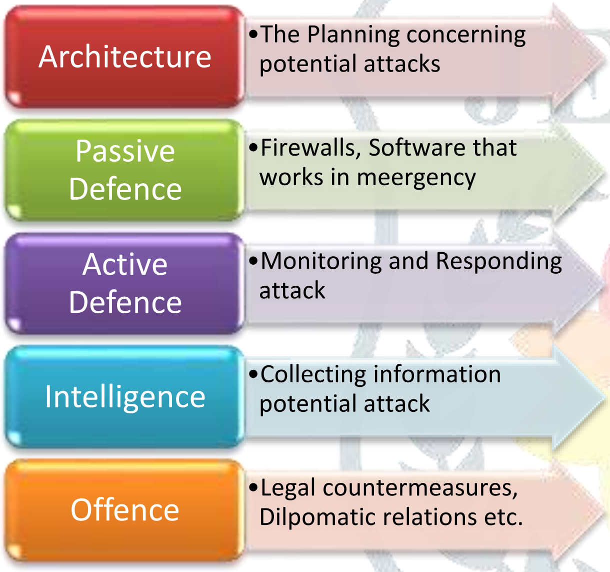
Architecture
•The Planning concerning potential attacks
Passive Defence
•Firewalls, Software that works in meergency
Active Defence
•Monitoring and Responding attack
Intelligence
•Collecting information potential attack
Offence
•Legal countermeasures, Dilpomatic relations etc.

Figure 6: Defence Mechanism of a cyber-attack

Architecture Level defence: Proper architecture would dictate the ability to segment or disable activities such as remote connections, and unnecessary outbound communications, while conducting active defence mechanisms. The infrastructure procurement must make sure that network elements have been tested as per International Security Standards such as BIS a standard IS 16335: 2015 for power control systems; ISO or IEC 15408 and ISO 27000 series standards for Information Security Management System. Vulnerability and Penetration test should also be carried out for both Main and Back-up system during factory acceptance test. Third party investigation can also be carried out for more layered protection. Properly segmentation of networks from each other should be done so that if one segment is infected other is not. It should be ensured that network switches are designed to capture data from the environment to support Passive and Active Defence mechanisms. A backup of critical software installers can help restore the system once the control is retrieved. A priority system should be developed from the most critical assets in the organization to least critical in order to best defend the critical infrastructures. The remote connections should be limited as less as possible; only to personnel who need it. In case of personnel need remote access, only specific to domain conformation should be shared. Two-form verification on the remote connections could help secure the system in better way.

Passive Defence Recommendations: In procurement procedure testing following provisions may be incorporated. Institutional framework should be developed for ensuring compliance of legal, contractual and technical framework to make the system very secure. The bidding documents should be so framed so as to encourage only firms which are manufacturing equipment in India to participate in the bid, including certification from the supplier that the equipment is “Safe to Connect”. Additionally, properly tuned firewalls between network segments will give visibility into the environment and allow defenders the time required to identify intrusions. A central logging and data aggregation point can be established to allow forensic evidence to be collected and made available to defenders. A password reset policy can be framed in the event of a compromise especially for VPNs and administrative accounts. An updated antivirus should be assured for endpoint security. An intrusion detection system should be deployed so that rules can be quickly deployed to search for intruders.

Active Defence Recommendations: The defenders must be trained to look out for abnormal or odd communication messages (such as new Internet Protocol communications) received or send from the power system infrastructure. A continuous network security monitoring should be put in place. Plan and train to incident response plans that incorporate both the IT and OT network personnel. An active cyber defence models for security operations should be deployed. Backup and recovery tools should be used to take digital images from a few of the systems in the supervisory environment such as HMIs and data historian systems every 6-12 months. This will allow a baseline of activity to be built and make the images available for scanning with new IOCs to catch emerging threats. The faulty section should be quarantined form the unaffected section as soon as possible and efforts should be made to restore the possible systems as quick as possible.

Intelligence Gathering: Instruct nodal officers of power utilities/IPPs to identify their critical infrastructure and submit status to CEA (within 15 days). Collection of security policies & control implementation status from nodal officers of power utilities/IPPs should be provided. Nodal officers to conduct security audit, vulnerability assessment & penetration testing of the identified critical infrastructure. This also includes the studies of difference cases of cyber-attacks in past and draft rules to fight in such eventualities.

Offense: All the efforts must be pushed to know the perpetrators of any cyber-attack on power infrastructures. Depending on the possible legal options and diplomatic possibilities all perpetrators must be brought to book of justice. In case of foreign perpetrators

Conclusion

The pace of technological changes in the field of communication is a challenge to track and adapt accordingly. Since communication being backbone of any automation, the security challenge is seems to be aggravating in future. The cyber security in the power system automation, smart grid and demand side management based distribution is also a tough challenge. With the above discussion about possible modus operandi of cyber-attacks, learning from previous experiences and strategic planning and execution of this challenge can make the defenders upper hand over the attackers.

The plan laid out here cannot just help power system infrastructure but can also be deployed in pipeline security for large oil and gas infrastructures critical manufacturing, military linked industries, nuclear facilities and anywhere or everywhere automation exists.

References

[1] Energy Statistics India 2021, National Statistical Office, Ministry of Statistics and Program Implementation, Government of India.

[2] C. Kumar, V. Pandey, P. Seshadri, A. Gartia and P. Mukhopadhyay, "Statistical analysis of power system events in Indian grid," 2016 National Power Systems Conference (NPSC), 2016, pp. 1-5, doi: 10.1109/NPSC.2016.7858924.

[3] E-ISAC, white paper on “Analysis of the Cyber Attack on the Ukrainian Power Grid, Defence use case”, published by SANS – Industrial Control Systems, 18th March 2016.

[4] Utpal Bhaskar, Live Mint News. Available at https://www.livemint.com/technology/tech-news/52-of-indian-firms-fell-victim-to-cyber-attack-in-last-12-months-sophos-survey-11617089719022.html

[5] Staff Reporter, Live Mint News. Available at https://www.livemint.com/technology/tech-news/52-of-indian-firms-fell-victim-to-cyber-attack-in-last-12-months-sophos-survey-11617089719022.html