Smart Grid Security - Overview

Secure the Smart Grid from Cyber attack

Traditional electrical power grids are currently evolving into smart grids, this adds up the flow of information and data along with electricity. This concept has given the electricity providers an improved way to control flow of electricity across cities and regulated the flow of informational data.

This feasibility of controlling the electricity from IP networks has always attracted the adversaries from the dark side. Smart Grids are more prone to attacks because of its critical impact over the entire city(s). Traditional cyber-attacks are attempts made by adversaries from a remote location for sabotaging computer systems and networks. However, if it is possible for adversaries to alter the expected behavior of a power system or compromise sensitive information, minor consequences would incur instability of demand-response systems, while major catastrophes could be financial losses, physical destruction to the power systems and even human injuries.

Therefore, it is necessary to identify Critical Cyber Assets i.e., those Cyber Assets essential to the reliable operation of Critical Assets. The most targeted part in Smart Grids are its Control Networks and Management Controls. Basically, Control networks are those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site. The control network connects the supervisory control level to lower-level control modules. Similarly, Management Controls are the security controls i.e., safeguards or countermeasures for an information system that focus on the management of risk and the management of information security.

Smart Grid Cyber Security - Advanced threats

Smart Grid systems are not secure by default. As a result, Smart grids are inherently exposed to a host of internal and external risks that threaten the integrity of the Smart Grid environment and its sensitive data.

Cyber attackers are continuously trying to compromise Smart Grid networks across the world and are trying to hit the power supply. Recent compromises like Ukrainian Power outage has made the impact visible to all the countries. Hence, security is a must to prevent the existing posture of the organisation from different attack scenarios.

Common Smart Security threat vectors:

- Default credentials in network devices
- Using vulnerable firmware device
- Insecure communication protocol
- Insecure authentication mechanism

- Configuration flaws like access rules, filtering of traffic in firewalls or other devices
- Vulnerabilities in web/mobile/desktop applications
- Flaws in Smart Meter vendor applications
- Segregation flaws due to misconfigured access rules at the intersection points
- Access to administration services

Mainly, Smart Grid domain is divided into seven subdomains – Bulk Generation, Distribution, and Transmission, customer, service providers, markets and operations. The vulnerabilities affecting these subdomains are mentioned below:

1. Bulk **Generation:** Also known as Distributed Control System. This is a local control system at a bulk generation plant. This plant consists of Field devices, Multiplexers, Field Bus modules, switches, Engineering/ Operator Workstations. The vulnerabilities affecting Bulk generation plants are:
    - Operating System related vulnerabilities in workstations
    - Vendor Application specific vulnerabilities
    - Communication protocol related vulnerabilities (like MODBUS has many known vulnerabilities)
    - Relaying Commands to tamper with field device parameters by performing MITM
    - Unauthorized access to devices/workstations
    - Improper access controls configured in switches/ firewalls
    - Insecure/weak remote access mechanism
2. **Transmission**: Transmission Control System involves the management of devices used to transmit status and measurement information from a substation or feeder equipment to a SCADA system and transmit control commands from the SCADA system to the field equipment. The vulnerabilities affecting Transmission system are:
    - Unauthorized remote access to RTU's
    - Use of Insecure Communication protocol (like IEC104) over the entire network
    - Denial of Service affecting SCADA system
    - Command Tampering
3. **Distribution:** Distribution Management System involves various actors like Distribution data collector, Distribution Automation field devices, Distribution Remote Terminal Unit, Distribution sensors etc. The vulnerabilities affecting the same are:
    - Unauthorized remote access to RTU's
    - Vendor based applications
    - Insecure communication protocol (like IEC104)
    - Command Tampering by intercepting the traffic between RTU’s and Operator Workstations

4. **Customer:** It involves the home appliances that interact with the meters or an interface between the distribution, operations, service provider, and customer domains and the devices within the customer domain. The vulnerabilities affecting the customer domain are:
    - Tampering with Smart meter parameters
    - Firmware related flaws
5. **Operations:** It involves Advanced Metering Infrastructure, Customer Information system, Customer service representative, Distribution Management Systems, Distribution Supervisory Control and Data Acquisition etc. The vulnerabilities affecting the Operations domain are:
    - Metering vendor applications
    - Flaws in services and protocols when Meters interact with application and database
    - Distribution Management Application flaws
    - SCADA vendor management applications
    - Third party devices to manage the logs and GPS connectivity
6. **Service Providers:** It includes Retail Energy providers- marketers, broker, public agency, city, etc. that combines the loads of multiple end-use customers in facilitating the sale and purchase of electric energy, transmission and other services on behalf of these customers. The vulnerabilities regarding the same are:
    - Applications (Web/mobile based) related flaws which the service provider and customer are using to create new connection or any billing related.
7. **Marketing:** It includes Energy Market Clearinghouse and Independent system operator/Regional Transmission Organization Wholesale Market which mostly deals with financial system. The vulnerabilities regarding the same are:
    - Financial related application security flaws

By following the NIST Smart Grid Security Guidelines **(NISTIR 7628)** we have developed a strategic approach to strengthen the overall security of Smart Grids which involves the following steps:

- ➢ Collecting the documented **information security policy and procedures** and verifying the implementation. This also involves improving overall security posture of an organisation.

- ➢ Reviewing the overall **Network architecture** of the organisation which involves Operational and Informational Technology networks. Enhancing the security by hardening the overall as well as various critical/intersection points of the two (OT/IT) networks. It also involves proper security assessment of any third-party devices added to the network like GPS system (Time server), Data logger devices for specific alerts/incidents etc.

- **Communication Protocols as well as insecure service protocols** used to communicate over IT/OT environment are given special attention while incorporating security. The insecure flow of data/commands can hit the entire demand-response system if targeted by the advance adversaries.

- Identifying the **vulnerabilities found in the system devices** connected to the internal network and providing recommendations regarding the same. This involves finding the flaws in user's devices, workstations, various servers, terminal devices, SCADA equipment, network/security devices etc.

- Identifying **configuration flaws in the network devices as well as in different workstations/servers**. Rules, access controls, traffic flow, policies etc., are verified after thorough understanding of the network architecture and appropriate recommendations are provided to resolve the issues found.

- Identifying the **devices exposed to public network** and finding the flaws regarding the same through external penetration testing. At the same time developing the security testing approach considering different scenarios.

- Identifying the **remote access mechanism** and finding the security related flaws as how the users or vendors are connecting to the control/enterprise network. Once the user gets the access to the internal network then reviewing the privileges that the user/vendor shall get.

- Identifying **security awareness gap** within the organisation and providing security awareness training to all the stakeholders. Various recent attacks are discussed and how the adversaries triggered it by targeting the stakeholders.

Smart Grid Cyber Security Assessment

Entire Smart Grid Cyber Security Assessment can be divided into 5-steps which provides an in-depth review of the Smart grid domain and the organization's ability to protect its most important information against cyber-attack.

Identify: Identify key assets in Smart Grid domain.

Assess: Assess existing Smart Grid architecture for advanced security threats using Smart Grid Cyber Security Framework and industry leading tools.

Secure: Provide industry leading solutions to secure the entire Smart Grid technology stack from cyber threats

Monitor: Develop target operating model to monitor and defend Smart Grid landscape against cyber threats

Smart Grid Cyber Security in 5 steps

- **Identify**
  - Identifying all the critical cyber assets that together form Smart Grid domain
  - Identifying the operational scenarios by interacting with respective stake holders
- **Assess**
  - Involves Blackbox/whitebox penetration testing of the entire network and field devices
  - Assessing the ICS communication protocols and method of communication (wired/wireless)
  - Reviewing the configuration of devices/servers
  - Review field device communications (wired and wireless)
  - Identifying trust relationships and interconnectivity with the enterprise network
  - Reviewing the Network architecture against known standards
- **Secure**
  - Analyze the results of Smart Grid security assessment and providing recommendations for the same
  - Prioritizing and ranking identified risks on the basis of their impact
- **Monitor**
  - Developing target operating model to monitor and defend Smart grid domain against cyber threats
  - Technologies and methods utilized for detecting anomalous activities
  - Monitoring the updates of all the critical cyber assets regularly as per compatibility
  - Upgrading the components or architecture as per advancement in technology

Case Study – Smart Grid Cyber Security Assessment

The purpose of this case study is to give an overview of how one can use this 5 step framework to test the Smart Grid security. This will give you an overall security approach and how this can be fitted to your Smart Grid domain.

In this assessment we covered the overall Smart Grid domain which includes all the seven major subdomains- service providers, customer, transmission, distribution, bulk generation, markets, and perations.

In the bulk generation plant, also known as Distributed Control System we assessed the entire architecture thoroughly. Some of the points are bulleted below:

- Communication between field devices and Control Processor
- Communication between Control Processor and DCS workstation(s)
- Security of Operating systems installed in DCS workstation(s)
- Application layer security
- Network devices security
- Interconnected network level security
- Physical security

Similarly, we follow our approach to assess other subdomains at each layer. As, in transmission and distribution network every component is assessed separately, which includes separate assessment of RTUs, Master/Backup Control Center, backhaul network, traffic analysis and other network equipment. The most important thing is that while assessing we do care about your critical devices. We just don't run scans blindly over the critical network. Transmission and distribution network is a group of many critical devices i.e. Smart Grid equipment and network devices, which makes it hard to manage all at the same time. Lot of vulnerabilities like default passwords in RTU, use of vulnerable communication protocol, device level vulnerabilities, application related flaws, configuration related issues etc. were discovered during the assessment.

In the Advanced Metering Infrastructure, all the components like Smart Meter applications and databases, communication path/hops and data transfer mode/protocol being used are keenly observed against threats. All the devices connecting these Smart meters to the Applications are thoroughly observed. So, while doing the assessment we discovered many vulnerabilities. Most of them were found in vendor based smart meter applications.

References

1. *http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf*