Security for Smart Grid Network

Priyanka Manve 2nd sem Mtech,
Department of computer science engineering
SJB Institute of Technology
Bangalore, India.
Priya.manve@gmail.com

Mrs.Rekha, Asso.Prof,
Department of computer science engineering
SJB Institute of Technology
Bangalore, India.

***Abstract* – A smart grid is a complex network composed of millions of devices and entities connected with each other. The virtual universal agreement to necessary upgrade the electric grid to increase overall system efficiency and reliability. Technology currently in use by the grid is outdated and unreliable. Old technology leads to inefficient systems, costing unnecessary money to the utilities, consumers, and taxpayers. To upgrade the grid and operate on improved grid will require significant dependent on distributed intelligence and broadband communication capabilities. The access and communications capabilities require the latest in proven security technology for extremely large wide-area communications networks. Supervisory control and data acquisition systems are used extensively to control and monitor critical infrastructure including power, gas, oil, and water. This paper discusses key security technologies for a smart grid system, public key infrastructures and trusted computing model, complexity of the smart grid network vulnerabilities.**

I. INTRODUCTION

Newly introduced capabilities for smart grid systems and networks are distributed intelligence and broadband capabilities greatly enhance efficiency and reliability and also create much new vulnerability if not deployed with the appropriate security controls. Providing security for such a large system may seem an unfathomable task and if done incorrectly can leave utilities open to cyber attacks. Standards from other systems and industries the best security solutions can be utilized for each portion of the smart grid communications network. The Internet-based protocols such as IPv4 andIPv6 which have been developed over many years and have widespread that will provide a cost-effective baseline transport. Layering the suite of. security protocols developed for on this baseline transport capitalizes on the vast work done in this area by protocol and industry experts While the smart grid system is made up of a number of energy subsystems many of the communications and security components are common between these energy subsystems. One subsystem which is at the core of smart grid systems is the Supervisory Control And Data Acquisition (SCADA) solution. Multiple vendors offer SCADA solutions which have varying capabilities and security mechanisms. Some standards exist are SCADA such as Distributed Network Protocol 3 Generic Object Oriented Substations Event, IEC 61850, and IEC 60870-5 still a need to make more consistent the security solutions applied to SCADA deployments. A second component key to smart grid systems is a number of secure, highly available wireless networks. These would include wide area, land mobile radio systems and broadband networks such as WLAN and WiMax. Third key element is a comprehensive security solution. Security solution for smart grid which heavily leverages public key infrastructure technology and trusted computing techniques. Supervisory control and data acquisition systems are real-time process control systems that monitor and control local or remote devices. They are extensively used in critical infrastructure including power, gas, oil, and water. A large number of modern intelligent electronic devices are installed in substation automation systems that provide powerful tools to collect, monitor, and analyze data. In a smart grid the devices provide valuable information that can be used to improve reliability and reduce operating costs. SCADA systems are secure as they utilized dedicated communication lines and proprietary protocols. Modern SCADA systems are being implemented using industry standard Transmission Control Protocol/Internet Protocol (TCP/IP) networks, different communication technologies, and SCADA protocols. To integrate IEDs in smart grid infrastructure, utilities are deploying SCADA systems as well as extensive communication networks including wireless access networks and IP networks in modern electric power systems.

Rapid increase in electric power demand, renewable energy mandates, and push towards electrification in the transportation sector is expected to increase power system. The standard security techniques in information networks, such as dedicated network or channel, intrusion detection systems third-party authentication and cryptography may not be applicable for SG wireless communication. The security requirements for smart grid and scale of the system and availability required we believe utilizing public key infrastructure (PKI) technologies along with trusted computing elements supported by other architectural components, is the best overall solution for smart grid. The most effective key management solution for securing the smart grid will be based on PKI technologies. PKI is more than just the hardware and software in the system. It includes the policies and procedures which describe the set up, management, updating, and revocation of the certificates that are the heart of PKI

The following are limitations:

A. Low cost

The cost is the first priority for the users and suppliers. To be cost effective, the computational power, memory and storage of the smart devices are limited. It leads to severe restriction on modern security techniques, such as:

- Complicated cryptographic algorithms may exhaust all computation and storage resource of units
- Third party applications, such as private key generator, may visibly increase the cost of whole wireless system

B. Low-bandwidth:

The communication channels in lower distribution and consumption grids are designed to transmit short message, and require only low bandwidth. Integrity protection mechanisms such as cipher-based message authentication code add typically 64 to 96 bits to every message. This leads to a high overhead in such a channel and might cause latency which is not affordable in many applications in SG. Distributed IDS can detect and classify malicious data and possible attacks by monitoring the communication traffics on many modules with doubled traffic flow might exhaust the bandwidth on these modules.

C. Easy-maintenance:

The wireless networks in SG should be flexible and easy to manage. It would be unrealistic to hire hundreds of engineers to manage users' encryption keys and change battery. Xia and Wang present that applying public key infrastructure (PKI) to SG requires significant work and maintenance of the public key management Under these constraints the ideal security method for SG wireless communication should satisfy:

- Applying simple algorithms that can be implemented with limited computational power, memory and storage
- Few or none additional communication burden
- Self-organizing, self-management and being independent of any third-party.

Security Requirements and Threats

Although the significance of specific threats can diverge depending on the assets that need to be secured some critical threats addressed in SCADA networks are as follows:

Bypass controls, spoofing attack, man-in-the-middle (MiTM) attack, modification attack, replay attack, insider attack, denial of Service (DoS) attack, and compromised user.

Key requirements that must be covered by a secure SCADA system are:

- Integrity — preventing unauthorized modification or theft of information
- Authentication and authorization —evading forgery/spoofing and unauthorized usage
- Availability — preventing DoS attack and ensuring authorized access to information
- Confidentiality — avoiding disclosure of information to unauthorized persons or systems.
- Non-repudiation/accountability — preventing denial of an action that took place or claim of an action that did not take place.

II. System Architecture

Based on the security requirements for smart grid the scale of the system and availability required utilizing public key infrastructure (PKI) technologies along with trusted computing elements supported by other architectural components is the best overall solution for smart grid. The most effective key management solution for securing the smart grid will be based on PKI technologies. PKI is more than just the hardware and software in the system. It also includes the policies and procedures which describe the set up, management, updating, and revocation of the certificates that are at the heart of PKI.

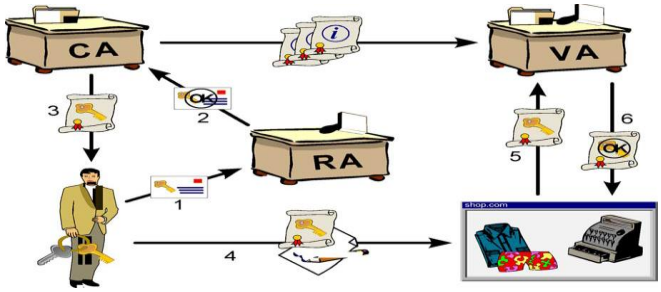

Fig. 1. Basic PKI procedure

A PKI binds public keys with user identities through use of digital certificates. The binding is established through a registration process where after a registration authority (RA) assures the correctness of the binding the certificate authority (CA) issues the certificate to the user. Users or devices can authenticate each other via the digital certificates, establish symmetric session keys and subsequently encrypt and decrypt messages between each other. The basic steps in utilizing a PKI are shown in Figure.1. The certificate subject, desiring communication with a secure resource begins by sending a certificate signing request to the RA. The RA performs vetting function which determines if the requested bindings are correct and if so signs the CSR and forwards it to the CA which then issues the certificate. When the certificate subject wishes to access a secure resource it sends the certificate to the RP. The RP validates the certificate typically by requesting the certificate status from a validation authority (VA) who replies in the positive if the certificate is valid PKI allows for a chain of trust and a first CAs extends trust to a second CAs by simply issuing a CA-certificate to the second CAs. This enables RPs that trusts the first CA to also trust subjects with certificates issued by the second CA. When two CAs issue each other certificates it is referred to as cross signing. CAs from one organization can extend trust to the CAs from other organizations enabling secure interoperability across domains. CA certificates can contain various constraints to limit the trust being extended by the issuing CA to the subject CA. In large systems PKI could be significantly more efficient than shared keys in terms of setting up and maintaining operational credential. The fact that each entity needs to be configured with its own certificate. This is compared to symmetric key provisioning where each device may need to be configured with a unique key pair for every secure link. While PKI is known for being complex many of the items responsible for the complexity can be significantly reduced by including the following four main technical elements:

- PKI standards
- Automated trust anchor security;
- Certificate attributes;

- Smart grid PKI tools.

Standards are used to establish requirements on the security operations of energy service as well as smart grid device manufacturers. Certificate policies used for issuing certificate formats, and PKI practices.

Trust anchor security is the basis for all subsequent trust relationships. But often trust anchor management mechanisms are as simple as trusting the IT administrators to install the correct certificate for the root CA in all RP devices with little efficiently verifying the correctness of this operation. For systems with thousands or hundreds of thousands of nodes an efficient and comprehensive trust anchor management system is needed.

Certificate attributes provide an important component to achieving the high availability needed for the power grid. We need to ensure incorporation of security and device authentication does not unnecessarily impose or extend service outages, due to unreachability of a security server. Thus entities must carry their complete credential with them in the form of an attribute certificate or certificate contains sufficiently detailed policy information to allow an RP to determine the applicability of the certificate holder to a given service.

Smart Grid PKI Standards

PKI is a powerful tool that can be used to provide secure authentication and authorization for security association and key establishment. PKI can be y difficult to deploy and operate. Primarily PKI standards only provide a high level framework for digital certificate usage and for implementing a PKI. Example they do not specify how a particular organization should vet certificate signing requests how the organization should protect each CA. They provide a mechanism for defining naming conventions, certificate constraints, and certificate policies, but they do not specify how these should be used.

Trust Anchor Security

One major component of a secure PKI enabled system is the requirement that each RP must have secure methods to load and store the root of trust or trust anchor (TA). The TA is typically a CA at the top of a CA hierarchy. RPs trust certificate holders because they trust the TA which trusts a CA which trusts the end certificate holders. Trust is evidenced by a chain of certificates rooted at the trust anchor. If an adversary could change the root of trust for any RP, that RP could be easily compromised.

Certificate Attributes

Smart grid to continue to function and other portions of the grid infrastructure are unreachable it will be essential for smart grid devices to be able to authenticate and determine the authorization status for each other without the need to reach a back-end security server. To do this two additional capabilities would be required. First, smart grid certificates will require policy attributes to indicate the applicability of the certificate to a given application. Second a local source of performing certificate status will be required.

Smart Grid PKI Tools

Standard smart grid operators would have to familiarize themselves with PKI concepts terminology and risks. Standards alone may not necessarily provide a cost-effective solution. Given set of standards it would be possible for vendors to develop smart grid PKI tools which are based on these standards. Tools would greatly ease the process of managing the PKI components needed to support the smart grid application. These tools will be knowledgeable of the appropriate smart grid certificate policy and certificate format standards and are used to programmatically enforce compliance to those standards. Such tools will enhance interoperability reduce the burden of running the PKI and ensure that appropriate security requirements are adhered it is reasonable to expect that the cumulative vulnerability of the system may also be vast. Virtually all parties agree that the consequences of a smart grid cybersecurity breach can be enormous. New functions such as demand response introduce significant new attack vectors such as a malware that initiates a massive coordinated and instantaneous drop in demand potentially causing substantial damage to distribution, transmission, and even generation facilities.

Considering the incredible size of the threat and wide-ranging potential consequences from cyberattacks the smart grid cybersecurity protection requirements must be extreme. The grid will require a comprehensive security plan that encompasses virtually all aspects of grid operations. One component of such a plan includes trusted computing platforms. Basic trusted computing model. platforms and associated mechanisms are used to ensure that malware is not introduced into software processing devices.

There are two categories of devices for which the malware protection problems should be considered: embedded computer systems and general purpose computer systems. Embedded systems are computer systems that are designed to perform a specific task or set of tasks. They are intended to run only software that is supplied by the manufacture. General purpose systems are intended to support third party software purchased by the specific consumer who purchased the system. A PC is an excellent example of a general purpose system. A microwave oven, or cable television set-top box are examples of embedded systems. Thus problem of malware protection should be considered separately for each category.

For embedded systems the problem of protecting the system against the installation of malware can be solved with high degrees of assurance. First manufacturer must implement secure software development processes many standard models for such processes are defined in. Second if the device is intend to be field upgradable the manufacturer must provide a secure software upgrade solution. The predominant method of doing this is to manufacture the embedded systems hardware with secure storage containing keying material for a software validation. The hardware is

configured with the public key of a secure signing server operated by the manufacturer. The device can validate any newly downloaded software prior to running it. The proactive approach can provide higher levels of assurance than can be obtained with a reactive approach such as a virus checker.

Additional security can be obtained by validating the software each time the device boots up. Such techniques are referred to as high assurance boot. HAB techniques typically rely on core software in secure hardware to validate boot-block code. The boot-block code then validates the operating system and the OS in turn validates the higher level applications. Each validation step is performed with public key or keys preinstalled in the secure hardware.

For devices which are intended to run for long periods of time without booting it is useful to have a method of performing secure software validation on running code. It is possible to have background tasks that can periodically perform such functions without disrupting the operations of the device. It is further possible to couple such background validation steps with other operational aspects of the device, such that if the device is found to be compromised, secure hardware on the device needed to bring up and maintain security associations with remote entities will prevent the local device from establishing and maintaining security associations with the remote entities.

Device attestation is needed to ascertain the devices on the network, true identities, ahead of any manual or automated provisioning at the site. Device attestation techniques accredited manufacturers can factory install device attestation certificates in each smart grid device. These device attestation certificates are used only to assert the device manufacturer, model, serial number, and that the device has not been tampered with. These certificates coupled with the appropriate authentication protocol can be used by the energy service provider to ensure that the device is exactly what it claims to be. In order to support device attestation the device

Attack Case In Smart Grids

A micro smart grid platform is constructed in our lab to investigate how the attacker intercepts the communication of smart meter and injects bad data into smart meter.

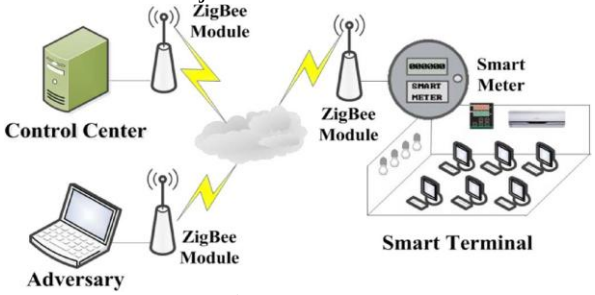

Fig. 2 Experiment platform.

Micro Smart Grid Platform

Micro smart grid platform is established consisting of three sides: Smart Terminal (ST) Control Center (CC), and Adversary. ZigBee is applied to build wireless network in the platform. IEEE 802.15.4 standard defines Fig.3 Experiment platform the physical and MAC layers of ZigBee, while the ZigBee Alliance defines the network and application layers. Since it is designed as a low cost, low rate, low power and low complexity personal area network, ZigBee is considered as an ideal protocol for smart grid applications, such as real-time system monitoring, load control, and building management In platform CC2430-F128 demo board is applied to design the ZigBee Module for wireless communication. CC2430-F128 chip is a system-on-chip solution specifically tailored for IEEE802.15.4 and ZigBee applications.

On the ST several smart meters (SIEMENS SERTRON PAC4200) are applied to monitor a micro power grid including various electronic devices. SIEMENS SERTRON PAC4200 is a power monitoring device for displaying, storing, and monitoring all relevant system parameters, such as voltages, currents. In present experiments 12 parameters: voltage, current, active power, and apparent power on three-phase, are selected to monitor and report. Several computers are deployed as the CC and Adversary. CC ZigBee module is set as normal mode to communicate with ST. The Adversary is set promiscuous mode to eavesdrop the communication between the ST and CC.

Smart Grid Attack Cases

Most terminal devices in smart grid are connected into intranet as smart sensors and intelligent applications. It is believed that the malicious users could not access them without the intranet and mac address of these devices. The Adversary obtains the address of the smart meter by monitoring their communication and then injects the false data into the meter. The Adversary can capture the packet sent from ST. The application protocol is Modbus which is widely used to connect the supervisory computer with the remote terminal unit in industrial network such as supervisory control and data acquisition (SCADA) systems.

Vulnerabilities

Smart grid network introduces enhancements and improved capabilities to the conventional power network making it more complex and vulnerable to different types of attacks. These vulnerabilities might allow attackers to access the network break the confidentiality and integrity of the transmitted data and make the service unavailable. Following vulnerabilities are the most serious in smart grids:

- Customer security: Smart meters autonomously collect massive amounts of data and transport it to the utility company, consumer, and service providers. This data includes private consumer information that might be used to infer consumer's activities devices are used and times when the home is vacant.
- Greater number of intelligent devices: A smart grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points into the network. Massiveness of the smart grid network

(100 to 1000 times larger than the internet) makes network monitoring and management extremely difficult.

- Physical security: Unlike the traditional power system smart grid network includes many components and most of them are out of the utility premises. Fact increases the number of insecure physical locations and makes them vulnerable to physical access.
- The lifetime of power systems: Since power systems coexist with the relatively short lived IT systems it is inevitable that outdated equipments are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices.
- Implicit trust between traditional power devices: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. Device sending a false state makes other devices behave in an unwanted way.
- Different Team's backgrounds: Inefficient and unorganized communication between teams might cause a lot of bad decisions leading to much vulnerability.
- Using Internet Protocol (IP) and commercial off-the-shelf hardware and software: Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. Devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service.
- More stakeholders: Having many stakeholders might give raise to a very dangerous kind of attack: insider attacks.

Proposed Solutions

The major vulnerabilities and security challenges for security solutions are :

- Identity should be verified through strong authentication mechanisms. Organizations should implement an implicit deny policy such that access to the network is granted only through explicit access permissions.
- Malware protection on both Embedded and General purpose systems. Embedded systems are intended to only run software that is supplied by the manufacturer. The manufacturer is required to embed in its products a secure storage that contains keying material for software validation. The system can validate any newly downloaded software prior to running. General purpose systems are intended to support third party software. For this system up-to-date and frequently updated antivirus software along with host-based intrusion prevention are required.
- Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS) technologies should augment the host-based defenses to protect the system from outside and inside attacks.
- Vulnerability assessments must be performed at least annually to make sure that elements that interface with the perimeter are secure.
- User actions can open potential system vulnerabilities. The awareness programs should be put in place to educate the network users about security best practices for using network tools and applications.
- Devices must know the sources and destinations they communicate with. This is accomplished through mutual authentication techniques using Transport Layer Security or Internet Protocol Security .
- Devices should support Virtual Private Network architectures for secure communication.
- Devices must use Public key Infrastructure to secure communication. There some constraints regarding cryptography and key management. current devices do not have enough processing power and storage to perform advanced encryption and authentication techniques communications in smart grid system will be over different channels that have different bandwidths and connectivity where all devices certificate authorities and servers must be connected at all times.
- Huge amount of transferred data utilities should only collect the data needed to achieve their goals.
- Control system and IT security engineers should be equally involved in securing the smart grid network.
- Since the life cycle of the smart grid is longer than that of the IT systems involved all IT technologies should have the ability to be upgraded.
- Security must be part of the smart grid design. Security of devices becomes vendor specific, fact that might produce much vulnerability because of incompatibility issues.
- Utilities should consider utilizing third party communication companies. The utilities handle all the grid communication becomes quickly a burden that the utility cannot handle. Third part companies can help in managing the communication and security issues of data transfer.
- A robust authentication protocol is needed while communicating between smart grid parties. The protocol must operate in real-time abiding with some constraints such as minimum computational cost, low communication overhead, and robustness to attacks especially Denial-of-Service attacks.

III. CONCLUSION

As a critical infrastructure element smart grid requires the highest levels of security. A architecture with security built in from the beginning is necessary. The smart grid security solution requires a holistic approach including PKI technology elements based on industry standards and trusted computing elements. To achieve the vision put forth in this paper there are many steps which need to be taken. Primary among them is the need for a cohesive set of requirements and standards for smart grid security .We urge the industry and other participants to continue the work that has begun under the direction of NIST to accomplish these foundational

steps quickly. The proper attention must be paid to creating these requirements and standards, as they will be utilized for many years given the lifecycle of utility components. We have proposed a lightweight and efficient substation-level security solution that provides multilevel multi-factor authentication and attribute-based authorization.

Traditional power systems are moving towards digitally enabled smart grids which will enhance communications, improve efficiency, increase reliability, and reduce the costs of electricity services. The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber attacks. The smart grid is considered a critical infrastructure, vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level. In this paper the vulnerabilities in smart grid networks, the types of attacks and attackers, the challenges present in designing new security solutions and the current and needed solutions.

REFERENCES

[1] Anthony R. Metke and Randy L. Ekl "Security Technology for Smart Grid Networks"

[2] Binod Vaidya, Dimitrios Makrakis, and Hussein T. Mouftah, University of Ottawa "Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Network"

[3] Ting Liu, Member, IEEE, YangLiu, YashanMao, Yao Sun, XiaohongGuan, Fellow, IEEE, Weibo Gong, Fellow, IEEE, and Sheng Xiao" A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication" IEEE TRANSACTIONS ON SMART GRID"

[4] Fadi Aloula*, A. R. Al-Alia , Rami Al-Dalkya, Mamoun Al-Mardinia,Wassim El-Hajjb" Smart Grid Security: Threats, Vulnerabilities and Solutions"

[5] Aaron St. Leger, Member, IEEE, John James, Senior Member, IEEE, Dean Frederick, Senior Member,IEEE" Smart Grid Modeling Approach for Wide Area Control Applications"

[6] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of A Smart Grid Infrastructure," IEEE Trans. Power Delivery, vol. 25, issue 3, July 2010, pp. 1501–07.

[7] S. Fries et al., "Security for the Smart Grid — Enhancing IEC 62351 to Improve Security in Energy Automation Control," Int'l. J. Advances in Security, vol 3, no. 3–4, 2010, pp. 169 83.

[8] B. Vaidya, D. Makrakis, and H. T. Mouftah "Provisioning Substation- Level Authentication in the Smart Grid Networks," Proc. IEEE MILCOM 2011, Nov. 2011, pp. 1189–94.