Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8160



Research Paper | Engineering

Topology for Smart Grid Security

Mr. Hitesh B. Kapadiya Lecture, Government Polytechnic, KHEDA, Gujarat,

Mr. Vinod S. Tejwani Lecture, Govt. Poly., Rajkot,

ABSTRACT

The security of any future Smart Grid is dependent on successfully addressing the cyber security issues associated with the nation's current power grid. Smart Grid will utilize numerous legacy systems and technologies that are currently installed. Therefore, known vulnerabilities in these legacy systems must be remediated and associated risks mitigated in order to increase the security and success of the Smart Grid. The implementation of Smart Grid will include the deployment of many new technologies and multiple communication infrastructures. Much of the technology currently in use by the grid is outdated and in many cases unreliable. There have been three major blackouts in the past nine years. Further, the reliance on old technology leads to inefficient systems, costing the utilities and tax payers unnecessary sums. There is virtually universal agreement that it is imperative to upgrade the electric grid to increase overall system efficiently and reliability. Such upgrades will require significant dependence 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. This paper discusses the key components for a secure Smart Grid system.

KEYWORDS :

1. INTRODUCTION

The smart grid promises a more efficient way of supplying and consuming energy. In essence, the smart grid is a data communications network integrated with the power grid and collects and analyzes data about power transmission, distribution, and consumption—all in near-real time. Based on this data, smart grid technology then provides predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power. At the heart of the smart grid is integration of the data communications networks of the generation, transmission, distribution, and customer components of the electrical grid. Increased connectivity presents many benefits, including giving consumers greater ability to control their power consumption and their energy bills. The smart grid also gives distribution and transmission grid operators more visibility and control over power supply, source, quality, and costs. Increased connectivity also presents challenges, especially in security. Because of the critical nature of the technology and the services it provides, the grid becomes a prime target for acts of terrorism and vandalism. Therefore, the transformation of traditional energy networks to smart grids requires an intrinsic security strategy to safeguard this critical infrastructure. As a result, a security vision must include a sound design for proactive security as well as resilience in the event of a security breach. Furthermore, a cyber security plan is crucial to receiving Department of Energy grant funding for smart grid projects. The Energy Department's Office of Electric Delivery and Energy Reliability has made it clear that even grant awards that score 'A' grades on all aspects but cyber security may not be approved. This paper describes vision and activities to ensure a secure smart grid and a reliable, sustainable energy supply.

2. CHARACTERISTICS OF SECURE SYSTEM

Let us assume that Alice is in the Human Resources (HR) department of an organization and Bob is an employee of the same organization. Alice is writing an official letter informing Bob about his promotion. What are the aspects Alice would be concerned about? She would be concerned that some unauthorized adversary would be able to access the contents of the letter. We describe this as confidentiality of the secure system. Alice achieves confidentiality by putting the letter in Bob's mailbox. Since only Bob has the key to the mailbox, nobody has access to the letter. As a receiver of the letter, Bob is concerned about three aspects. Firstly, the letter has actually been written by Alice. Bob assures himself by checking Alice's signature. We call this the authentication characteristic of the secure system. Secondly, if Alice had delegated somebody to put the letter in Bob's mailbox, then Bob is concerned that the other person may have tampered with the letter. To make Bob feel assured, Alice puts a seal on the letter. If anybody opens the letter the seal would be broken and Bob would immediately come to know that somebody had tampered with the letter. This is called message integrity. Thirdly, Bob can be concerned that Alice may later say that she had not given him that letter. However, since the letter has been signed, Alice cannot deny writing such a letter. This is called the non repudiation requirement of a secure system. Non repudiation works at different levels. Let us assume Alice delegates the responsibility of dropping the letter to Charlie. However, Charlie loses the letter. If Charlie had signed in a register mentioning that he picked up the letter then he cannot later say that he was not assigned the responsibility. This simple example illustrates that every day we have confidentiality, authentication, integrity, and non repudiation embedded into our systems. To make a computer system secure, all the above characteristics need to be followed. The characteristics are achieved in the same way as described in the above example, only the mechanisms are different.

3. SECURITY THREATS

Let us revert back to the above example where Alice writes a letter of promotion to Bob. Let us also assume that Bob has an adversary Derrick who wants to tamper with the process of Bob getting the promotion letter. What can Derrick do? He can prevent the letter from reaching Bob's mailbox by stealing the letter from Charlie. In this case, he resorts to interruption. Though different mechanisms can be employed, interruption is the most difficult threat to prevent both in computer and non computer systems. Another malicious activity that Derrick can resort to is to read the contents of the letter. If he is able to do that then he has resorted to interception. Interception does not always imply interruption. Derrick may actually read the contents, reseal the letter, and then put the letter in Bob's mailbox. He may be able to do this without raising any alarms. The third type of threat that any system would try to protect itself from is fabrication. In this case, Derrick writes a fabricated letter and puts the letter in Bob's mailbox. Derrick may not fabricate a new letter but may modify the contents of the old letter. Another type of threat which some systems may be concerned about is called replication. In this type of threat, the attacker does not modify or fabricate any message but replays or replicates the old message. If

the above example, if the letter contains one line "Bob, you have been promoted," signed by Alice without any date, then Derrick can store the previous year's letter and put it in Bob's mailbox this year. One may find this type of letter unreal and the threat impractical. However, this type of threat is really dangerous in many computing system where some amount of synchronization is required based on the received message. One such example is routing updates and creation of routing tables in the Internet scenario.

4. DIFFERENT ENCRYPTION SCHEMES

Encryption involves hiding the actual information so that any unintended receiver would not be able to decipher the contents of the information. Traditionally this has been carried out by performing a mathematical operation on the part of the information using a key which is a set of characters known only to the sender and the intended receiver.

5. UNIQUE SECURITY CHALLENGES

The smart grid is unique in several ways that present significant security challenges:

- Scale: The communications infrastructure necessary to support the global power grid has the potential to be larger than the Internet.
- Legacy devices: Unlike corporate IT systems that typically have a life span of three to five years; many devices in the smart grid have service lives measured in decades.
- Field locations: The power grid contains millions of field devices, such as meters, transformers, and switches. While physical security of these field devices is an important design consideration, the fact that they are potentially vulnerable requires that network security design not rely on them for grid integrity.
- A culture of "security through obscurity": Today's grid security often assumes that if the location or access method of a vulnerable point isn't widely known, it won't be exploited. Some people believe that the smart grid data communications network will be secure if it is built with proprietary, non-routable protocols, which would make it more difficult to access than a standards-based network. In reality, vulnerabilities cannot remain hidden for any length of time. History has shown that public availability of security algorithms that are subject to peer review has increased the security of these systems. Some examples are the Advanced Encryption Standard (AES) cryptographic standard, Diffie-Hellman asymmetric encryption keys, and the Internet Engineering Task Force (IETF) IP Security (IPSec) security standard. Flaws are discovered and resolved more quickly than in proprietary systems.
- Evolving standards and regulations: In this early phase of smart grid implementation, vendors are implementing security controls using a variety of standard and proprietary mechanisms. This leads to poor interoperability and difficult management. Early efforts suffer from a lack of independent testing and from frequently insecure implementations.

7 DATA CENTER SECURITY AND THE SMART GRID

As mentioned earlier, the smart grid will capture and analyze real-time data about individual customer energy usage patterns. This will enable customers to adjust their power demands, and will enable utilities to adjust the power supply and design services to better meet customer needs. Such massive amounts of information require not only more data storage than utility companies have ever managed, but also the highest security to prevent unauthorized use and ensure safe, timely disposal in compliance with regulations.

8. CONCLUSIONS

In this paper, we have looked at the different concepts and technologies that are useful in the grid computing context. Most secure systems look at providing confidentiality, authentication, integrity, and non-repudiation to the end users. Confidentiality is generally provided by encrypting the messages using symmetric or asymmetric encryption mechanisms. The former uses public/private keys for encryption purposes and the latter uses symmetric shared key between the sender and the receiver. Different types of authentication schemes include shared secret based authentication, public key based authentication, and third party based authentication mechanisms. Smart Grid security is as critical to the future of electric power delivery as Smart Grid functionality. Vendors, regulators and utility personnel have a shared responsibility to ensure that Smart Grid networks do not place utility operations at unnecessary risk, and that Smart Grid networks are operated in a manner consistent with sound security practices.

REFERENCES

[1] Grid computing Security by Anirban Chakrabarti|[2] Smart Grid Security Technology Anthony R. Metke and Randy L. Ekl Motorola, Inc., Schaumburg, IL USA|[3] www.Cisco.com|[4] www.currentgroup.com |[5] ibid., Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements