A Security Framework for Smart-Grids

Martin Andreoni*

* Grupo de Teleinformática e Automação, UFRJ - COPPE/PEE - DEL/Poli, Rio de Janeiro – RJ – Brazil
Email: martin@gta.ufrj.br

***Abstract*—It is known that actual electrical grid is suffering change to become a new Smart Grid with thousands of metering devices connected through telecommunications given intelligence to the grid. Having communication between the gadgets, will take in several cases the possibility of having the same attacks suffered in a normal network, such as Denail of Service (DoS), Man-In-The-Middle (MitM),etc. This paper will show a recompilation of methods to make a security framework focusing in the virtual authentication, with the objective of develop a future work in Security of Smart grids.**

I. Introduction

The depletion of global fossil fuel reserves in addition to the ever increasing environmental pollution have strongly impelled during last decades the development of renewable energy sources (RESs). The need of having available sustainable energy generation systems for replacing gradually conventional ones requires the improvement of structures of energy supply based mostly on clean and renewable energy resources [1]. In this aspect the smart grid is designed to replace the traditional the grid electric work making it more efficiently, securely and reliably through bidirectional flows of power and communication. The Smart grid is an upgrade to power generation and distribution that will let our energy network diagnose and heal itself, dynamically integrate renewable energy and local power sources and automatically lower electricity demand. The source of those new superpowers is information technology. However, increasing automation and communications within the electricity grid potentially has a dark side allowing increased vulnerability to attack. In order to deploy the two-way communication, one possible solution is to use advanced metering infrastructure (AMI) that contains a key component in the smart grid system called smart meter. A smart meter usually has a processing chip and a nonvolatile storage so that it can perform smart functions like being able to report periodic usage updates to end-users as well as the generation facilities at power company and interact directly with "smart" appliances at home to control them[2]. While a million of smart meters are being installed, numerous security challenges and issues for smart grid network have come out. The meter might be installed in front of a house and protected by physical lock devices, as a result, it is possible that a hacker breaks the lock, compromises a smart meter, and controls electrical appliances at home. In order to make this upgrade, it is necessary to take into account the need of being a smooth transition, in which several equipments in the actual grid are not ready to act as a virtual nodes, lot of them have mechanical parts that work slower compared with the elements shown in a normal network so is difficult to implement virtual security. However, not only virtual attack will the meters suffers, the global idea has to be make a framework in which physic and virtual security are involved. It is not necessary of being so extremist saying that the most secure network is the one which is not logged to the network, the concept should be implement a group of methodology to evaluate the whole security aspect. This paper will show a recompilation of methods to make a security framework focusing in the virtual aspect with the objective of develop a future work in Security of Smart grids, besides it will propose a method to make authentication.

A. Organization of the Paper

The rest of the paper is organized as follows. In Section II, reviews of the Architecture of the Smart Grid. In Section III, a review of commons attacks. Then in Section IV, it will show the related works, in Section V will describe the proposed system. Finally, the paper will conclude in Section VI.

II. Smart Grid Architecture

Dehalwar, Khole [3] has developed a conceptual architecture for Smart Grid. This conceptual architectural as depicted in Figure 1 that divides the Smart Grid into seven domains namely customers, markets, service providers, operations, bulk generation, transmission and distribution for information exchange and smart decisions. The home area network (HAN) provides access to in-home appliances while the neighborhood area network (NAN) connects smart meters to local access points, and the wide area network (WAN) provides communication links between the grids and core utility systems. Nevertheless, a conceptual security model must include three important security concepts: security-by-design, security-in-depth, and end-to-end security. Security-by-design relates to the manufacturing of individual products, and assembly of systems, solutions, and architectures. It consists of designing them from scratch with security in mind, as opposed to adding security features to an already built product. Security-in depth implies the realization that any security feature by itself is breakable with enough effort, and only multiple security barriers layered in a concentric way around protected assets can provide a security level superior to the sum of the individual parts. End-to-end security relates to the fact that the security of a network is as strong as it weakest link. Therefore, network administrators have to maintain the same level of security in all segments of the network. In addition, all the security should be

apply in all aspects to the network, applying excessive control in the SCADA layer and a hybrid model cyber-physical in the lowers layers.

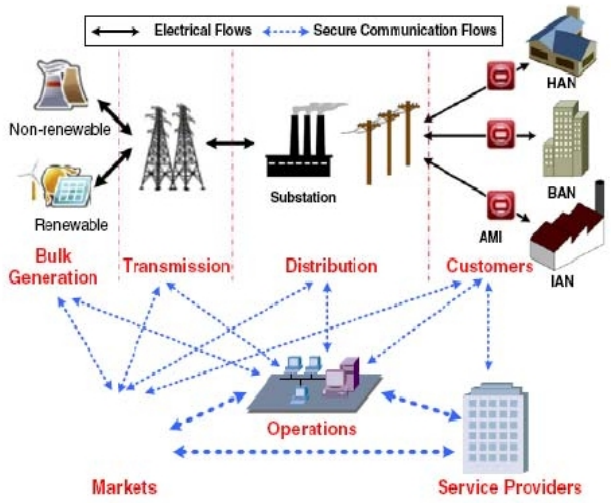

Figure 1. Architecture Smart Grid

III. Smart grids attacks

How was mentioned before the grid connected to the network could suffer several kinds of attacks, Chen, Cheng, and Chen, in [4] introduce three main attack categories and their countermeasures in smart grid communication networks.

•Vulnerability attack: This type of attack is induced by the malfunction of a device or communication channel, or the desynchronization of feedback information. Feedback information may be deteriorated by erroneous data delivery or unreliable channel conditions, which leads to an incorrect control process at the control center. The vulnerability attack is mainly caused by the inherent reliability in the communication network instead of malicious attacks with specific attempts, and it can be prevented by introducing the fault diagnosis scheme to infer thefault detection and localization.

•Data injection attack: This type of attack alter the measurements of some meters in order to manipulate the operations of the smart grid. Although the integrity of meter data and commands is important, their damage is mostly limited to revenue loss. In addition, countermeasures with which it is possible to defend against malicious data injection if a small subset of measurements can be made immune to the data injection attacks.

•Intentional attack: If an adversary is able to have full understanding of the network topology,it can fully utilize the network structure to disrupt the network operations by paralyzing some fraction of nodes with the highest degree. Intentional attack can be implemented via coordinated denial-of-service (DoS) attack and contributes to network disruption due to node disconnections in the communication network. From a graph-theoretic point of view, an intentional attack on a specific node is identical to node removal on the corresponding network graph. Intentional attack is quite effective in disintegrating the network and it is relatively difficult to be detected since the adversary attacks only some central but not all nodes in the network.

IV. Related Works

Several research have been done in the area of security in Smart Grids. Most of them are focused in attacks but none of them propose a complete security framework to avoid possibles attacks.

1) The case of IPV6:

[5] has presented the strategy and procedure of security checks and authentications of commands requests for operations in the host AEPS and interconnected multiple neighboring area electric power system (AEPS). Case studies of the new security management and authentication for smart grids operations for improvement of stability conditions due to contingencies.

In[6] it is propose a proactive defense based in IPV6, in which the Smart-Grid make robust against incoming exterior attacks, the method is called Moving Target IPV6 Defense (MT6D). One of the limitations that this work presents is the fact that is not possible to work with a dynamic allocation address. Moreover it work over IPV4 creating a tunnel giving huge latency to the system.

In the case of [7] They propose a simple a Security architecture of smart distribution grid data communications network which is divided in layer for better management. It is proposed a Three-Dimensional scheme including the network security, terminal security and application security, three parts, develop four levels of security research, environmental security, equipment security, network management information security, and network management information content security This is only a proposed architecture to split the security management in a smart-grid, and in [8] it is proposed a implementation of an IPV6 addressing but it is not focus on the security aspect.

2) The case Key Management:

In the case of the key management some works are directly oriented to the smart-grids in [9] he made a review those requirements and evaluate current PKI trust models, recommending adaptations toward a Smart Grid PKI that will meet the Smart Grid cyber security needs. The method proposed is a Hierarchical PKI Trust Model. In this work is not cited what happened when the system goes down.

Wu and Zhou present a solution to key management scheme for the smart grid but show that this is not secure against the man-in-the-middle attack. Their proposal is a scheme that contains three major mutual authentication schemes between different components including the collector, the aggregator, and the sensor in the smart grid. Like an authentication scheme in a Kerberos system, a trusted third party (e.g., trust anchor) is involved in the process of authentication as well. Them Man-in-the-Middle attack is solved by [2] in which They propose a scheme for a smart grid using a trusted third party which not only has no issue on key revocation, but also the third party can be easily duplicated in case power outages occur,

they call their protocol SKDP, according to them it is better that the combination of PKI and Kerberos.

V. Proposed System:

It is imagined a future scenario of the smart grid in which all the houses will have smart meters and the communications will be based in the Internet Protocol and Ethernet technology with Gateways to communicate with some others protocols such as ZigBee, which are in lower layers like sensors networks. This scenario was shown in 1. The authentication mechanism is based on Kerberos, it is built on public key cryptographic, but in this case it is going to be used the asymmetric public key cryptographic during certain phases of the authentication. The main idea is to authenticate all the Advanced Metering Infraestructures (AMI). To avoid the DoS attack the system will be provided with a Dynamic Host Configuration Protocol (DHCP) based on Internet Protocol Version 6 (IPV6). In case of need of having authentication or any other type of query without the presence of the network (off-line) it will be necessary the requirements of a smart cards to access the system itself, so the authentication in this case will be the serial number of each device, that should be certificated by the manufacturer as a genuine devices, taking away whom belongs to the Smart meter.

A. Election of the Authentication System

The actuals protocols implemented in the SCADA sistems nowadays like Distributed Network Protocol 3 (DNP3) were not built with security in mind, and seldom is IEC 62351, which is the security standard for these protocols, implemented. Moreover, The trend with the small sensors in the Smart grids is to make tiny devices with limited storage, low power, and bandwidth. This is a big problem with the PKI authentication method, in which the Certification Authority (CA), must carry with all the revocation certificates in the Certificate Revocation List (CRL) during the validation period of the certificate , and will be a huge amount of data to transfer each time that is requested, it would not be possible to manage for the small gadgets. Online certificate status protocol (OCSP) is alternative to the (CRL) of the PKI, and it offers an online revocation service from a trusted OCSP responder. With OCSP, the smart meter just needs to send a request to the responder and get an ”Ok”, ”Bad”, or ”Unknown” response. But OSCP still have some limitation if it is applied to the smart grid, OSCP servers must work online, so all the devices must be logged all the time. In addition OCSP requires that all the responses need to be signed digitally causing probably Denied-of-Service (DoS) in an intentional attack. These are some of the decisions why was kerberos chosen as a authentication system. Moreover, how it was mentioned before the servers of kerberos should be divided to serve all the huge grid. This will act as back-up or redundant workstations in case of natural disasters, etc.. Serving one of the concepts in Smart Grids, the reliance.

B. Kerberos

Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal. Kerberos optionally provides integrity and confidentiality for data sent between the client and server. Regarding to the terminology, the session key encrypted with the resource server's master key is known as a “ticket.” A Kerberos ticket provides a way to transport a Kerberos session key securely across the network. Only the destination resource server decrypts it[10]. It is necessary to have at least one kind of servers in the network, but according to the smart grid distribution could be necessary to have more than one in several hopes, giving in addition back up. In figure 2 it is shown the Kerberos authentication scheme.

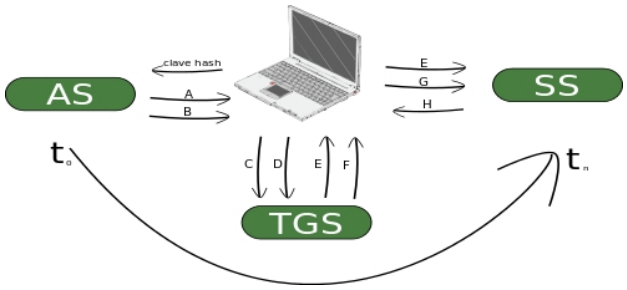

Figure 2. Kerberos Authentication Service

AS = Authentication Server
TGS = Ticket Granting Server
SS = Service Server

1) Encryptation:

Encryption in the present implementation of Kerberos uses the data encryption standard (DES). It is a property of DES that if ciphertext (encrypted data) is decrypted with the same key used to encrypt it, the plaintext (original data) appears.

2) Kerberos Issues and Open Problems:

There are a number of issues and problems associated with the Kerberos authentication mechanism. Among the issues are how to decide the correct lifetime for a ticket, how to allow proxies, and how to guarantee workstation integrity. Single point of failure: It requires continuous availability of a central server. When the Kerberos server is down, no one can log in. This can be mitigated by using multiple Kerberos servers and fallback authentication mechanisms. Moreover, Kerberos has strict time requirements, which means the clocks of the involved hosts must be synchronized within configured limits. The tickets have a time availability period and if the host clock is not synchronized with the Kerberos server clock, the authentication will fail. The default configuration requires that clock times are no more than five minutes apart. In practice Network Time Protocol daemons are usually used to keep the host clocks synchronized. The administration protocol is not standardized and differs between server implementations.

Since all authentication is controlled by a centralized Key Distribution Center (KDC), compromise of this authentication infrastructure will allow an attacker to impersonate any user. Each network service which requires a different host name will need its own set of Kerberos keys.[11][12]

C. IPV6

Nowadays, it is believe that using IPv6 on every device is an important step towards creating a controllable and interoperable grid energy infrastructure. When every device can publish data and be directly addressed globally, real time monitoring and control becomes possible and more sophisticated as other parties can easily interact with it over Internet and integrate its functionality. Additionally the user is in control over which data to share, with whom and for what purpose (e.g. with the energy providers for billing), as well as which policy should be used when conditions change. According to this, IPv6 Internet is considered as the next-generation internet protocol and satisfies the requirements of large-scale WSNs due to obvious advantages in the address space, addressability, security, mobility, QoS support, etc. In addition, it is an standard available and developed. Moreover it has a huge scalability that is one of the keys, because it will have millions of devices connected to it. thinking in future in the smart grids. According to the scalability IPV6, which uses 128-bit addresses, or 2128, and provides for far more available IP addresses than IPV4. It's also got a bunch of other advantages, including an easier way for devices to auto-configure their own addresses and a built-in mechanism for data security. The decision about using IPV6 in the smart grids is supported by several advantages of this protocol.[13] Open and standard based, lightweight, versatile, ubiquitous, scalable, manageable and secure, stable and resilient, just to mention some of them.[14] According to the security aspect, it has a lot of contribution made on it, thousand of attack, with their solution have been applied. For sure, it will inherit all the pros and cons of his predecessor the IPV4, but this is are not bad news, it has a lot of work development, research, etc. for more than 30 years.

1) DHCP for IPV6:

The basic DHCPv6 client-server concept is similar to using DHCP for IPv4. If a client wishes to receive configuration parameters, it will send out a request on the attached local network to detect available DHCPv6 servers. This done through the "Solicit" and "Advertise" messages. Well known DHCPv6 Multicast addresses are used for this process. Next, the DHCPv6 client will "Request" parameters from an available server which will respond with the requested information with a "Reply" message[15].

To summarize, the adoption of IP based networking for all Smart Grid services allows all devices involved in the delivery of these services to be managed through a single network view. All devices and the relationships between them at the IP level can be defined in the network management application and the impact of a failure of communication to any given device can be instantly evaluated and displayed. The typical DHCP behavior is shown in Figure 3.

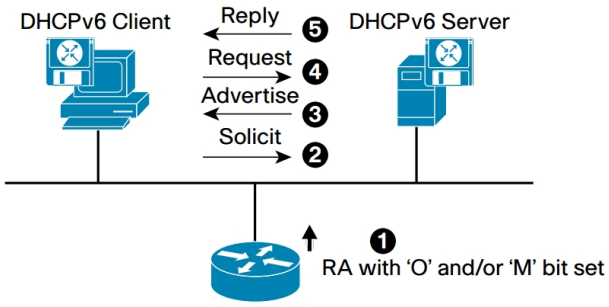

Figure 3. DHCP scheme

D. Smart Cards

A smart card contains a secure and tamper-resistant microprocessor chip. It has secure memories, serves cryptographic functions, and contains security applications. A recent trend is to make a smart card in a USB token form, which looks very much like a USB memory stick from the outside. To use it, a user plugs the smart card token into a USB port of a computer. The a smart card is divided into two main logical components - Host Agent and Card Agent. The host agent is the client software, which runs on the host computer. It enables Human Interface (HI) to the smart card as well as interactions with other programs on the host computer and remote servers. The card agent resides and runs inside the smart card. It keeps sensitive user data in its secure memory and performs cryptographic operations that access the data[16]. To support the Transport Layer Security (TLS) for HTTPS, the smart card maintains a RSA key pair and an x.509 certificate for host agent's web server. It keeps the private key in its secure memory, and stores the certificate and the public key in a MSD partition visible from the host computer. In this way, the web server can easily get the certificate during TLS handshaking. To achieve performance and maintain security, the host agent implements the TLS protocol in collaboration with the smart card. During the TLS handshaking, the host agent does computationally intensive work, including computing digest and generating session keys; the smart card does security critical parts, including decrypting the premaster secret (PMS) using the private key. Once the handshaking completes, the browser and the web server in the host agent communicate securely using HTTPS.[17] This is going to be the way to authenticate in case of the servers go down or need of being open a smart meter for someone authorized.

VI. Conclusions and Future Work

The presented system has been shown as an alternative for a implementation in the case of authentication in smart grids. As a future work we propose to test the kerberos system and compare it with some others authentication services such as

SKPD, RADIUS/AAA, PKI. Moreover test the DHCP of IPV6 under a testbed.

ACKNOWLEDGMENTS

This work was part of the Subject CPE728 Autonomia e Segurança em Redes directed by Professor Otto Carlos Muniz Bandeira Duarte

REFERENCES

[1] "Implementation of Wireless Remote Monitoring and Control of Solar Photovoltaic (PV) System" Martín E. Andreoni López, Francisco J. Galdeano Mantiñan, and Marcelo G. Molina

[2] "Secure Key Distribution for the Smart Grid" Jinyue Xia and Yongge Wang

[3] "Multi-Agent based Public Key Infrastructure for Smart Grid" Dehalwar, Khole

[4] "Smart Attacks in Smart Grid Communication" NetworksPin-Yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen. IEEE Communications Magazine August 2012

[5] "Computer Network Security Management and Authentication of Smart Grids Operations" Alexander Hamlyn, Helen Cheung, Todd Mander, Lin Wang, Cungang Yang, Richard Cheung

[6] "Using an IPv6 Moving Target Defense to Protect the Smart Grid" Stephen Groat, Matthew Dunlop, William Urbanksi, Randy Marchany,and Joseph Tront Innovative Smart Grid Technologies

[7] "Research on IPv6 Transition Evolvement and Security Architecture of Smart Distribution Grid Data Communication System"

[8] "Research on Transmission Data System of Smart Grid based on IPv6 DiffServ Model" Yang Ting Zhang Zhidong Wu Jiaowen Li Ang

[9] "Adapting PKI for the Smart Grid "Todd Baumeister

[10] "Public-Key Cryptography Enabled Kerberos Authentication". Sufyan T. Faraj Al-Janabi and Mayada Abdul-salam Rasheed College of Computer University of Anbar Ramadi, Iraq

[11] "Kerberos: An Authentication Service for Computer Networks"B. Clifford Neuman and Theodore Ts'o (September 1994).IEEE Communications

[12] "Kerberos Overview: An Authentication Service for Open Network Systems". Cisco Systems date=19 January 2006. Retrieved 15 August 2012.

[13] "Three-dimensional Location-based IPv6 Addressing for Wireless Sensor Networks in Smart Grid" Chih-Yung Cheng, Chi-Cheng Chuang, Ray-I Chang

[14] "A Standardized and Flexible IPv6 Architecture for Field Area Networks Smart Grid Last Mile Infrastructure", Rob Kopmeiners, Jeff Fry, Manager, Cisco Systems. December 2011

[15] "DHCP for IPv6" Cisco Systems. March 2009

[16] "Infrastructure Standards for Smart ID Card Deployment"Rick Kuhn, Susan Ladau,Ramaswamy Chandramouli,

[17] "A New Secure Communication Framework for Smart Cards" H. Karen Lu, Asad M. Ali, Stephane Durand, and Laurent Castillo. IEEE 2009