EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems Research Article ICST.ORG

Smart Grid Attacks and Countermeasures

Eric McCary, Yang Xiao*

Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290 USA

Abstract

The term “Smart Grid” has been coined and used for several years to describe the efforts of the current power grid modernization effort. This effort plans to introduce self-healing, energy efficiency, reliability, and security using two-way digital communications and control technology, along with a host of other valuable attributes. As a bi-product of this modernization and newly gained systems interoperability, new communications and management interfaces are produced in both the cyber realm and physical domains. The increase of the public physical presence and cyber footprint opens up avenues for compromise to hackers and individuals with malicious intent. This survey paper will categorize and summarize vulnerabilities in the framework of the current power grid and the software and hardware which is currently being used to upgrade the grid. The paper will also detail known countermeasures which can be used to mitigate or eliminate attacks which exploit such vulnerabilities.

Keywords: Smart Grid, Security, Attacks, Countermeasures

Received on 27 December 2014, accepted on 28 December 2014, published on 25 February 2015

doi: 10.4108/ inis.2.2.e4

1. Introduction

The smart grid can be described as a physical and cyber upgrade of the current power grid which will allow it to diagnose and heal itself, to dynamically integrate renewable energy from various sources to relieve dependency on centralized generation, and to provide the customer more control over electricity demand and cost [1]. The National Institute of Technology and Standards (NIST) defines six key areas which make up the grid below: bulk generation domain, transmission domain, distribution domain, operations domain, service provider domain, and customer domain [2]. Each domain houses several major components in the energy field and likely will have a unique distributed computing environment, sub-domains, and equipment to suit its mission-specific needs. It is also important to note that the domains of the grid are interconnected with adjacent domains which provide coordinated functionality. This also creates opportunity for advancement in resources and technology optimization, while also creating new areas of concern that have not been evaluated in the grid.

We can visualize the modernized grid as having two separate layers which will make up a complex cyber-physical system. This manner of description combines the current power grid which is composed of generation, transmission, and distribution [3], and a cyber-communication layer for each of the power grid’s domains which will then be connected and integrated with measures for useful interoperability. Each of these domains must have physical and cyber interfaces to allow for proper communication between devices connected to the grid which depend on mass aggregation of customer and equipment operational data.

These changes to the power grid infrastructure not only add intelligence and new communication technology, but will also create interfaces to select power systems and devices from open networks which may be facing the internet [1, 4, 5]. As this new technology will drastically increase efficiency and reliability, it also substantially increases the potential for vulnerabilities in the power grid [6-10]. Designers of many legacy devices in the grid with networking capabilities neglected the need for cyber security, and failed to consider these devices being widely connected [11-12]. Some of the devices employ embedded Web services and mobile interfaces which are becoming increasingly popular among vendors to service customers in providing them with energy information, and this makes target environments more vulnerable.

More efficient management of active grid devices can result in sizeable financial savings for the customers and utilities. Also, this management of energy will allow for

*Corresponding author. Email:yangxiao@ieee.org more efficient energy generation and distribution. The widely connected grid is integral to modern society, and generation and consumption must remain mostly balanced as it is produced and consumed. Potential cascading failures and power outages are possibilities if this condition is not met. The integration of previously separate portions of the grid incidentally interconnects legacy devices and software in the grid and implements current technology and smart devices alongside these devices. Some of the more modern equipment employs current software such as Windows operating system components as well as vendor created solutions which allow for advanced operations necessary for smart grid operation, but also creates vulnerabilities unique to those systems or, in other cases, widely known to the public and which may be exploited in the grid environment [13-14].

With the level of scalability and interoperability that a smart grid maintains, it is important to understand the physical and cyber ramifications that are a possibility with lacking standards and security implementations. Without these, as one study points out, attacks and other misfortunes on the grid will likely lead to cascading failures and power outages [15]. To convey a context for understanding this necessity, this paper will give a review of past attacks and vulnerabilities of the smart grid and also inspect and highlight some areas for additional research which may reveal other weaknesses.

Recent work in this area includes [3], which utilized a custom cyber-security testbed architecture in order to detail attack and mitigation scenarios within that simulated microgrid environment. These scenarios utilize common hacking tools to exploit vulnerabilities while mitigation is attributed to anomaly-based Intrusion Detection Systems (IDS) and firewalls. The authors in [6] give an overview of the relevant cyber security and privacy issues along with some recommendations proposed by NIST and other recent works. The authors in [16] summarize some of the requirements and vulnerabilities of the current grid including many of the protocols and common practices as well as vulnerabilities and challenges are detailed well. The authors in [17] present a review of the work related to guaranteeing availability in smart grid communications, and a common communication topology is detailed in which privacy compromising attributes are discussed. The authors in [18] supply the reader with some attack categories, and some security fundamentals in the areas of access control, authentication, and privacy along with intrusion detection are also discussed.

Recent work in this area has failed to give detailed accounts of techniques which exploit these issues and vulnerabilities in the smart grid and its technologies. Therefore this paper will cover these malicious actions and their impact on the grid and its components. Countermeasures will also be discussed.

Although the paper is about smart grid, the similar issues also happen in industrial applications. Many of the problems and solutions discussed in this paper can be used in industrial applications.

The remainder of this paper is as follows. First a description of the physical and cyber layer infrastructure will be given along with its components in Section 2. Section 3 will discuss some of the major security concerns plaguing the smart grid. Sections 4 and 5 contain attacks and countermeasures, respectively. Section 6 details attacks that have been reported in the public domain, while Section 7 discusses future plans and the conclusion of this work.

2. Background

In order to more efficiently handle the large amounts of data produced by the smart grid scheme, new hardware and software are designed to extract and manage this data. Also, smart devices are developed in a manner conducive to smart grid purposes. While discussion of the these intelligent devices are necessary due to the grids advanced functions, equipment for generation and transporting energy will be included below.

2.1. Power Grid Physical Infrastructure

In order for the basic operations of a smart grid to be completed in a power grid, specific equipment must be strategically placed in or nearby the regions being serviced. The physical infrastructure of the smart grid can be described as the hardware that will support the functionality of the energy generation, transmission, and distribution mechanisms. The physical entities present on the smart grid are a combination of advanced hardware designed for frequent monitoring of the grid systems and interconnected devices including their load and resources in real-time. In addition to management and measurement devices, the grid must maintain hardware to carry out its known functions of generating energy and transporting it.

Bulk generation is the first of the responsibilities of the grid. In this domain, power generation plants play a major role as they generate the energy and are overseen by control systems. The interconnection here with the transmission networks is necessary to move power from its initial location to remote distributors across the entire service area.

Centralized generation stations typically rely on coal, nuclear, natural gas, or hydroelectric methods to achieve mass energy levels for transmission [17]. Also, solar and wind energy may be used for specific purposes. Large turbines are used and propelled by combustion to produce energy used, along with fuel burning engines, photovoltaic panels, and various other generation technologies. Other integral portions of the generation stage include the cooling systems and furnaces/boilers. Energy produced in this sector is moved along transmission lines across transmission domains.

The U.S. power grid is made up of roughly 200,000 miles of transmission lines [11]. These lines act as a vehicle for providing distribution networks with power.

Table 1 includes some of the major hardware located in the transmission domain works together to achieve its goal. This will help us understand this mechanisms' operation.

Table 1: Common Grid Hardware [2,12]

Transmission Hardware	Description
Transmission Lines/Towers	Serves as transmission level energy vehicle
Substations	Transforms, Regulates Voltage
Control Hardware (Switches, Breakers, Loads)	Controls Flow of Electricity
Transformers	"Transforms" energy between voltages
Capacitors	Energy storage
Supervisory Data and Command Acquisition (SCADA)	Monitors and controls industrial process
Phasor Measurement Unit (PMU)	Measure electrical waves
Data Collector	Collects data

Normally, voltage must be regulated while moving into the lines for more efficient transmission. The transmission networks, like all other smart grid networks, have interconnections and divisions which can each be categorized as servicing their respective grids. This division allows for increased efficiency and more reliability in individual grids. Micrograds may be included here, which include localized efforts which encompass the generation, transmission, and distribution domains on a smaller scale. Electricity travels over the transmission lines as alternating current (AC) with transformers adjusting the current, stepping it up or down as the current moves into separate portions of the transmission network as necessary.

A typical power grid is composed of power stations on both the generation stage and between the transmission and distribution stages, power lines which serve as a vehicle for the either distribution or transmission class power, and transformers to step the power voltage up or down as necessary.

The smart grid will upgrade this infrastructure to support two way communication and flow of power. Also, equipment is upgraded for advanced sensing and measurement. These items include PMU, SCADA, and Advanced Metering Infrastructure (AMI) [5].

This equipment has the task of providing the key functionality which is established by Federal Energy Regulatory Commission (FERC) in its policy statement including: efficiency and demand response (DR), situational awareness spanning wide areas, storage of energy, PHEV (Plug-in Hybrid Electric Vehicles), communication networks, AMI, and distribution grid management [2].

The distribution network is composed of distribution class power lines which are used to supply consumers with power of a lower voltage. This power is delivered once it is stepped down by distribution transformers which transform the voltage down to a level for use in homes and businesses. In this domain, the AMI resides. The AMI affords the grid and power consumer DR, load management, real-time pricing, and distribution automation through the network topology visualized in Figure 1 [13].

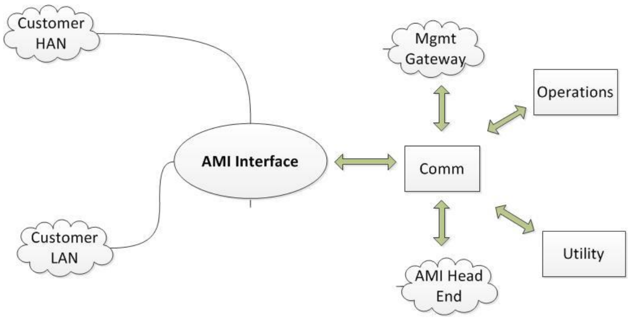

Figure 1. Simple AMI Communication Architecture [13]

The endpoints of the AMI normally reside in the customer domain providing for many advanced capabilities due to their accessibility to the customer. Intelligent Electrical Devices (IEDs) located in the residential or commercial areas which are connected to the AMI, allow the customers to modulate energy load based on the necessary DR signals or their economic ability or pre-established requirements or preferences. AMI portals are widespread and utilized on a by vendor basis and allow customers access to their energy usage and pricing information. These interfaces also introduce vulnerability to the smart grid infrastructure.

Other entities important to the grid that spans across domains include transportation infrastructure such as roads and bridges. While a great amount of automation is possible in the smart grid, it is still important in some situations to deliver physical service to outlying hardware in the field. Methods to effectively travel to these points in sufficient time to repair equipment are important to grid operation. Buildings and intermediary housing units also play a role in the grid.

2.2. Power Grid Cyber Infrastructure

The cyber layer of the grid is integral as it is where gathering and analysis of real-time data occurs. Consumers, power system operators, ISOs, and producers all utilize this layer of the grid to accomplish various tasks. This data normally contains sensitive information whose availability, integrity, and confidentiality must be retained in order for the proper operation of the grid and its resources. The major parts of the cyber layer of the grid extend from the transmission level down to the distribution level. Figure 2 demonstrates this:

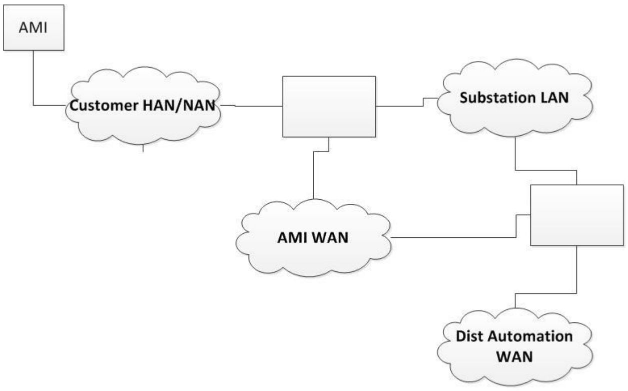

Figure 2. Simple Smart Grid Communication Architecture

This layer is composed of several interconnected networks and must communicate across boundaries. As the paper [19] states, many of the connected networks are of a hybrid nature. This means that networks may be composed of differing methods of connectivity such as Wi-Fi communications and satellite. Also, in these integrated networks, there will exist an endless variety of differing requirements, legacy systems, and cutting-edge technologies which direct the future trends in the smart grid systems. This has led to difficulty in establishing a universally adopted set of standards [6, 20-21].

Integration of Internet Protocol (IP) into grid networks is a major property of the smart grid. IP has become the protocol of choice based on its mature performance, security potential, and reliability [22]. IP will be the medium which smart grid devices use to communicate with each other [5]. Successful legacy system activity on the smart grid networks can be accomplished with the implementation of IP [23]. In other words, this protocol allows for encapsulation and many methods which can be used to allow two systems to communicate which normally utilize non-routable communications on a network or with a particular type of connection.

Currently there are many legacy devices still being utilized in grid networks which must communicate and may create vulnerabilities and other difficulties such as bottlenecks. As cost is always a factor, it is very likely that these technologies will continue to exist through the near future.

2.2.1 Monitoring and Visualization

As per the definition of a smart grid, the entity must have monitoring and sensing capabilities spread throughout. These modules acts as the “eyes and ears” of the grid which provide frequent diagnostic data from specific devices which can yield grid state information. Enhanced capabilities in sensing and monitoring allow for detection of anomalies in the grid, which then can be resolved by automation controls in the monitoring device software. Problems that require a more intensive solution by sending crews to physically manage affected devices or strategically re-route power and services.

Sensor technology is also important in the estimation of customer load [24, 25]. AMI technology on the utility side can be used to predict the times during the day that electricity prices will be at their peak. This gives customers the decision to curb their energy usage during those peak times. Less demand equates to lower peak prices and less energy waste for the whole energy sector.

Functionality provided by SCADA and Remote Telemetry Units (RTUs) allow for controlling and management of the transmission layer devices [8]. Many different types of sensors are currently in use on the smart grid architecture. A list of some of the technologies is located below: regulators, smart voltage sensors, smart capacitors, dissolved gas sensors (transformers), temperature sensors, line condition sensors, and weather sensors [26].

Once measurements are sent to the appropriate entities and verified, the results can be viewed on an Energy Management System (EMS) which may provide an interface to the control capabilities in order to make appropriate modifications to grid operations.

Devices such as the PMU sense and relay measurements to control centers where they are aggregated and compared to policy guidelines to determine whether or not action is necessary to ensure proper operation of the grid. This is one portion of the demand-response regulation procedure which keeps utilities from wasting money by having excess power wasted, or brown/black-outs from occurring due to too little power flow.

One method of sensing in the smart grid is to establish policy for state in the grid, and the specific bounds which encompass a “good” state, where measurements outside of these ranges signify a fault or intrusion on the grid. These system stability or state recognition readings may be the magnitude or phase angle recorded from a remote PMU which is relayed to a control center or substation for analysis and monitoring

2.2.2 Analytical Capability

The cyber layer in the transmission and distribution domain is responsibility for monitoring and analyzing state variables and preventing or correcting faults or predicted conditions in the grid. Stability analysis is the key in the grid as automation is one of the attributes expected in the architecture. As long as actions are defined in the policy which is specified in the grid, there should be no difficulty creating automatic response functions due to the state sensing and measurements in the grid.

The North American Electric Reliability Corporation (NERC) maintains a public list of reliability standards which helps to regulate and standardize cyber requirements in the US electric grid [27].

3. Security Concerns

The elements of the “CIA Triad” (Confidentiality, Integrity, and Availability) normally provide a good baseline for security in major operational systems. These same requirements exist in the smart grid, even more so than in the past. These automated systems which are also in control of human and equipment safety, help drive the grid to its main objectives.

In order to understand security differences in cyber-physical systems as opposed to traditional Information Technology (IT) systems, both cyber domain attacks, physical domain attacks, and crossing domain attacks should be accessed [28]. Methods from cyber domain, physical domain, and crossing domain should be used mitigate interactions among domains.

As one of the benefits and most integral attributes of the grid is its two-way communication which allow utilities and customers to relay data between each other on a real-time basis, it is imperative for these data transactions to be secured at all costs. This level of communication also creates vulnerabilities in grid communication with a broadened surface for cyber-attack and data tampering [29, 30].

Initially these protocols and the devices interfacing it were proprietary and detached from aces to outside networks. This basically suggests that grid networks employed “security by obscurity” instead of “defense-in-depth”. Normally the design of these networks and mechanisms implemented in them were not initially assembled or created with security in mind. As time has progressed, vendors have incorporated security into the device designs, and the protocols in use on smart grid networks have adapted to the malicious threats and individuals threatening critical infrastructure. A list of popular protocols in use on smart grid networks is included in Table 2.

Table 2: Common Grid Communication Protocols [2,19, 31]

Communication Protocol	Description
Zigbee 2.0	For use in HAN for device communication
IEC 61107/62056	Smart meter communication protocol
ANSI C12.	Smart meter and HAN device communication protocols
HomePlug	Suite of specifications for communication over home electrical wiring
M-Bus	Protocol for remote metering
Modbus	Standard for communication in industrial devices
OPC Protocols	Open standard specification for publish/subscribe procedure
DNP3	Substation device automation
IEC 60870	Outlines control messages
IEC 61850	Outlines communications between transmission and distribution domains in automation and security

In North America, Distributed Network Protocol 3 (DNP3) is used frequently in process automation for electric utilities. This protocol is built on top of IP and along with IEC 61850 and DNP3, which are currently the most widely used protocols [32, 33]. Open Connectivity (OPC) standard is an abstraction layer between separate components of which may implement different and incompatible protocols. Each of these protocols, regardless of popularity have been or will be used in operational settings and should be secured as so.

There are some obvious and interesting differences in the priority of security objectives in the smart grid and contemporary IT networks. The security requirements rely heavily on the domain under consideration in the grid. We first look at the CIA Triad and understand that the order of objectives here are different from those in the traditional IT network.

This is partially due to the personally identifiable information that is aggregated and communicated back and forth from consumer to utility over public internet channels, and the publically available resources in the field. Utility companies collect and store information belonging to the customer including name, address, consumption data, and social security number. Each of the attributes should be kept confidential and away from hackers attempting to affect them or the grid maliciously. While IT security techniques are valid and will be implemented in the smart grid in an effort that likely will satisfy security requirements, we must understand the tradeoff between security cost and performance to validate specific implementations.

3.1. Confidentiality

Confidentiality in the smart grid deals with restricting unauthorized explicit and implicit information dissemination. This may result from unauthorized access to a system or the network that it interfaces with, or an insider acquiring data with either malicious or unauthorized benign intent.

Data moving across smart grid networks contains power usage data and other private and sensitive information that can be detrimental to a consumer [14, 29]. Malicious attackers can infer specific details from power usage patterns and fashion an attack according to the details acquired from eavesdropping on the smart grid information network. This sensitive information may be sought after by many entities for instance, law enforcement could utilize this information to support investigations, not unlike the way that cell phone and Global Positioning System (GPS) data is currently used [32].

The paper [34] details and expands on work in [35, 36] which describes information flow in environments with multiple security domains. This complicates both the automation processes of devices in a smart grid network and security in these environments.

IEC 62351defines several mechanisms which are to be used to protect the exchange of information in automation applications used in the smart grid. IEC 62351-3 and 62351-5 provide provisions for confidentiality using Transport Layer Security (TLS) for encryption between devices in the network [35, 37]. Also these protocols adopt a keyed hashing message authentication (HMAC) as specified in IEC 9798-4.

3.2. Integrity

Integrity in the smart grid alludes to modification of devices or data on the grid infrastructure. Normally attacks of this nature are more difficult to accomplish, and require more sophisticated methods to implement. All attacks from network data injection, message replay, or masquerading violate integrity on a network. A less exploited vulnerability would be modifying the functions of hardware or software on devices before it is shipped from the producer, or modifying images that will be on machines in an operational environment. Malware can be pre-loaded and designed to propagate to other devices on a network. Also, hardware can intentionally be made to falsely read data, and/or malfunction under certain circumstances.

On the consumer's end, where the hardware is much more easily available, a wider range of vulnerabilities exist that can attack integrity. From data injection on a large scale, to AMI cyber-physical tampering, it is important to secure devices and networks on several levels in the cyber and physical layer to ensure integrity on.

Normally, due to the operation of the grid, attacks affecting integrity are hard to detect, and in the case of compromising meters and their load information in a coordinated fashion, these are the most prevalent [38-40]. These types of attacks involve stealthy modification of reports intended to inform utilities of resources usages. Changes can be made to deceive the utility into believing that the resident generated an untruthful amount of energy in order to reduce costs of their energy consumption. Whether theft or fraud, these acts can have devastating effect on the load estimation mechanism in the grid causing too much or too little energy to be produced and eventually failure of select nodes or blackouts.

3.3. Availability

Availability can be ensured if the smart grid services are protected and accessible to all entities requesting them. This attribute is centered on reliability and security of the features providing services. In the smart grid environment, availability itself is the most important of the immediate security objectives that should be completed in the grid. The critical nature of the grid and its services, along with the necessity of its real-time operation help explain the significance of the requirement of the grids constant availability. The paper [41] categorizes past research in availability as follows: defence against attacks, guarantee of real-time systems, and communication availability extension.

An important part of ensuring availability is to understand the threats posed to an environment. This way, it becomes an easier task to ensure the security of the systems that it is composed of. Once security is ensured, the reliability of the grid is placed solely on the internal function of the grid hardware and software barring acts of God.

The current grid provides a 99% uptime [42], and the near negligible amount of down time is caused by storms electromechanical arching, and other perturbances that are normally unavoidable. Most of these are physical concerns, but the smart grid upgrade creates vulnerabilities on the cyber side. Malicious control from the cyber side can easily disable systems in the grid and cause widespread downtime and blackouts.

3.4. Hacker's Motives

The heightened level of communications between customers and utilities creates more opportunity for eavesdropping. The paper [42] gives us motivation for individuals whether malicious or not, to attempt to hack the grid: intellectual stimulation, recognition of peers, power acquisition, terrorism, revenge, penetration testing, curiosity, and monetary gain.

The smart grid is not a target of attack for only terrorist and there will also be individuals with non-malicious aspirations attempting to access and perform acts that may have negative affect on the grid. These efforts can be carried out with a simple demonstration of power in mind, and end up causing millions of dollars in damage.

3.5. Known Vulnerabilities

While security controls continuously have been making exploitation of obvious and available vulnerabilities more difficult, the devices behind perimeter defences remained un-hardened up to acceptable specifications. Some of the challenges of upgrading the current grid are listed below [43]:

a) difficulty of creating security solutions in complex environment due to propriety nature based on performance and not security,
b) networking technologies including ModBus, ProfiBus, ICCP, ModBus Plus, and DNP being designed for connectivity and not security,
c) automation systems bring composed of legacy systems for the near future,
d) and fast addition of new protocols, applications, and requirements being more difficult to make and keep complex systems secure.

SCADA systems are an excellent example of this premise [8]. Previously utilized proprietary protocols and software were implemented on these devices rendering them vulnerable to common and easily executable attacks.

Therefore, it was believed that these obscure devices did not have any threats of note due to its unknown nature and unreachable state.

In the past, these SCADA systems hosted vulnerabilities such as programmed default password implementations, missing software patches, and network protocol-based vulnerabilities [44]. These types of vulnerabilities are normally of a vendor-specific nature, and have specially crafted exploit techniques.

Accidental and inadvertent threats are always of concern in any operational environment. These types of breakdowns may even cause more problems than actual vulnerability exploitation by a hacker. Insufficient safety procedures, equipment failures, and natural disasters are all of concern.

It is important to consider the fact that legacy systems will initially play a large role in the smart grid. While observing this fact more often than before, we understand that the smart grid must be defined not by all new hardware and software, but by the integration of legacy devices, protocols, and their two-way communication on as much of the current framework as possible while adding new equipment as necessary and financially permissible. This threat can stem from inadequate resources or configuration to implement sufficient security mechanisms in the devices. Several solutions are currently in use, including utilizing secure Virtual Private Networks (VPNs) for remote access, encapsulating the legacy devices, or creating and abstracted layer between the legacy device and the requesting service as an interface to reduce the complexity of actions necessary by the legacy device [44].

4. Attack Types

Any infrastructure is vulnerable to attack. Whether the vulnerability is great or small is determined by the mitigation and security techniques implemented around and within it. In the smart grid, specific elements and security requirements are necessary for operation.

Vulnerabilities can be described and categorized in many different ways. We can view the weaknesses of the smart grid on a device or entity basis or as a combination of those entities. A list of devices that have specific vulnerabilities and important purposes on the grid is listed below in Table 3:

Table 3: Vulnerable Grid Entities [2, 31, 42, 45]

Operational Systems	**IT Systems**	**Communication Protocols**	**Endpoints**	**Human Factors**
Generators	PCs	Wifi (IP)	Electric Vehicles	Human Training
Transformers	Servers	Zigbee	Smart Meters	Social Engineering
SCADA	Apps	4G	Mobile Devices	Phishing
PMU	DBs	DNP3	IEDs	Data Transfer
PLC	Web Services	IEC 60870		
Smart Meters		IEC 61850		

Most of the effective attacks affecting the smart grid are a combination of several of the vulnerable entities attached to it. Whether the goal is malicious or for testing purposes, normally the exploitation of highly valuable resources employing security mechanisms requires complicated procedure to complete. This could consist of a coordinated attack carried out in a distributed fashion and utilizing several different types technology and attack vectors.

4.1. Physical Attacks

The smart grids footprint is greatly extended to due to the interconnection of consumers' home and business networks to other information networks that link them with the control centers and substations. This requires equipment to be installed on consumer property which will likely be part of the AMI, which communicates power usage information and several other important pieces of data between dedicated data aggregation points or control centers and customers. Also, sensors and other advanced and costly hardware will be placed in publicly accessible areas which are vulnerable to attack.

Physical security is fairly mature and well understood, and while the list of types of physical attacks is relatively short, the possibilities are greatly expanded due to availability. Destruction of equipment and disturbance of availability is the prime objective here and requires a much less skilled individual to achieve when compared to a cyber-attack. This is a type of denial of service attack (DoS), and multiple DoS attacks create a distributed DoS (DDoS) attack. When implemented in this manner, the attack may cause incorrect data or false sensing and state readings, and ultimately malfunctioning equipment.

Transformers are normally located inside substations and also out in the customer domain while being easily recognizable and reachable. These are large and relatively stationary devices that are normally difficult to relocate and normally constructed outside of the United States.

Also, many smart grid components have a high monetary value which makes these publicly available components of the grid easy and expensive attack targets. The cost resulting from attacks of replacement of the equipment, and the service costs incurred by individuals completing the system repairs or replacement will normally lead to ill effects for the utility.

Attacks on physical infrastructure in the public domain can have significant effect on the smart grid as a whole. Black-outs and surge related damage of equipment can result from physical compromise of current managing or directing components of the grid.

4.2. Cyber Attacks

When determining specifications for cyber security in the smart grid, we must understand that legacy techniques are not sufficient in this environment [16]. Compared with networks in the regular cyber domain, smart grid networks and their devices have more complex objectives and assumptions on what needs to be protected [46]. Taking this into account, it is important to use current cyber security techniques only where they are sufficient, while discovering and implementing new methods elsewhere.

4.2.1 Attacks on Access Control

Access control is no new issue in environments composed of many systems and networks [47-49]. This field, like any other computing field, requires and allows multiple users to access information stored in databases or device storage. Access should be controlled for much more than just stored data, devices and networking environments should be included. The stored data may include calculating costs, predicting future load, and special case monitoring. Each of these sets of data must be sent to specific users while restricting access from un-authenticated users.

In the smart grid setting, there are several types of users which require access to data involved with the grid. These roles include operators, engineers, technicians, and managers [50]. The policy implemented in the systems must manage multiple domain and network architectures. The interconnection of domains and grids presents difficulties in current access control policies. The policies in question should exemplify good management attributes as explained in [51], including well protected credentials and policies. Neglect in the form of hard-coded credentials is vulnerability whether publicized or not.

Some of the mainstream methods used to protect this information fall under the category of attribute-based encryption (ABE) [52] or role-based access control (RBAC). These schemes can have their user revocation abilities bypassed if one gains the ability to masquerade or tamper with a legitimate user's attributes or communication stream. These basic schemes have been found insufficient as they cannot satisfy the requirements of secure authentication across multiple domains and the real-time necessity for communication in the grid [53]. Several vulnerabilities have been found implemented in IT networks that allow for exploiting access control in some capacity, including broken authentication, broken access controls, and information leakage [50,54]. These types of lapses are normally errors in policy implemented in a network. These schemes normally implement key distribution centers (KDC) in their architectures [55]. In the instance that the scheme utilizes a single KDC, this also presents a single point of failure. An attacker has the opportunity to carry out a DoS attack and stop legitimate users from accessing important data stored and accessed on the grid.

The paper [54] introduces HMAC combined with challenge-response method which follows the RBAC scheme. This is another situation which is susceptible to multiple vulnerabilities in the grid. An information and credential stealing session can provide a hacker with the data to masquerade and gain access to secret of sensitive data. In many instances, proper encryption is not in place in networks vulnerable to man-in-the-middle attacks.

Several vulnerabilities have been discovered in equipment from specific vendors which allow for access to backdoors in SCADA systems. These backdoors have included valid credentials being hardcoded into an operational system's software which allows for trivial means of access by a hacker [56, 57].

4.2.2 Attacks on Cryptography

According to [58, 59], the cryptography flavor of choice for the smart grid is that of a public key infrastructure (PKI). This means that each of these networks have well-known vulnerabilities. This method creates a vulnerability in which a single point of failure exists between a key distribution agent or certificate authority (CA) when utilizing a certificate-based system. A successful DoS attack would render all or most encrypted communication invalid or foreign as the receiver does not have the ability to verify the sender's identity. In addition to a single point of failure, vulnerability exists in a hacker's ability to acquire the root key in a PKI which would allow for unfettered malicious communication [60] as modern masquerading techniques are advanced and sufficient [61, 62]. The network administrator is responsible for creating policy which will require a new root key in a sufficient time cycle and have adequate detection systems to mitigate or alert monitoring installations of intrusions or key stealing.

Legacy equipment's lack of compatibility with newer standards is also an issue. Smart grid networks such as SCADA networks must interface with many devices new and old. When an un-hardened legacy device is reachable via outside network, it presents liability not only to itself, but to the entire network behind it.

In a smart grid system, where the real time nature is critical, all traffic with sensitive data should be encrypted. Even though this is so, traffic can still be analyzed in order to infer specific attributes of the systems. With the use of any high level encryption techniques, it becomes infeasible to retrieve the actual sensitive data from the raw data packets, but it is possible to intercept timing and frequency information of the messages in order to deduce information from the network which the malicious individual would like to attack. Then the analyzed metadata contained in the message information belonging to the sender can be used to exploit specific inferred vulnerabilities [42].

4.2.3 Attacks on Firmware/Software Policy

A method used with many devices hosting modern software is automatic online updating. This process is normally utilized to upgrade a device's firmware or version of software to the latest version. While this functionality is crucial in AMI and in devices in other sub-networks, its implementation may ultimately be the source of malicious acts. Some devices in the smart grid may have a prescheduled "window" of opportunity for upgrade which the device is hard-coded to adhere to [63]. This can allow a hacker the opportunity to load a malicious version of firmware or software onto the devices and allow for more devious acts from the inside.

Field devices with remote firmware/software capabilities may also allow for unrestricted operations during update [64]. In the instance of insufficient authentication measures implemented in the update process, an attacker uploading malicious software to a device may be able to modify functionality of the device or create methods to upload other malicious software at a later date.

In addition to malicious software/firmware uploading, meter cloning and meter migration are also threats [44]. Meter software can be stolen and uploaded into other hardware which would replace an actual meter and be manipulated however the hacker pleases. Malicious data or processes may also be injected into the software before it is installed on the meters in the manufacturing phase. Also, meters may be swapped with neighboring units which previously have recorded lower energy usage than the meter designated for the property designated to use the meter being replaced. This will cause an incorrect reading and pass this false data to other smart grid mechanisms.

4.2.4 Attacks on Network Design

Network architectures that future systems will be modeled after will most likely resemble a mesh-like topology [51, 65,66]. This type of system will of course be placed on top of the existing power grid infrastructure. The end-users, such as households and businesses, will communicate their power usage and pricing data with local area utilities which collect and process data from smart meters and PMUs, pass that data on to aggregation points, and finally deliver the data to a substation or back-end network. The design of the network must support the key smart grid services explained earlier whose benefits are targeted for both utilities and customers.

DoS attacks are of great concern here. In the case of natural disaster or malicious physical attack in area which there is lacking redundancy and fault detection. These DoS attacks can be of a distributed nature in which Internet Protocol (IP) addresses are spoofed, flood the victim network, or be a single attacker that attacks a specific service or grid component. This may result in blackouts or rolling brownouts and network overloads [67]. The mesh network topology allows for redundancy and reduces repair costs as the grid is to be resilient in failure and the recovery for most situations should be automated.

The designs must support distributed generation and bi-directional energy flow which are both integral attributes of the smart grid.

4.2.5 Software Input Validation

We can describe vulnerabilities in software input validation as those dealing with the underlying software-related architectural concepts of the systems interconnected on the smart grid network. These types of vulnerabilities are not always caused by implementation design flaws, but many times by a protocol or standard which prioritizes other elements over security, and are affected on multiple levels. These vulnerabilities in the past have also been the product of web applications with automated functionality providing remote or internal access into the smart grid network. Some types of attacks include buffer overflows and java/web interface exploits [23].

A buffer overflow occurs when a program writing to a buffer in memory and writes more data than the size of the buffer and completes its writing in adjacent memory. In an environment in which this is allowed policy does not require for all input to be checked, such as customer data, grid component data, etc. An attacker can create false data and send this data to the substations as if it were a valid and authenticated entity. With a specially crafted message that takes advantage of a lack of standardization for instance, is larger than the typical message size and writes pass the buffer end on the receiving machine. At this point the attacker can execute arbitrary commands.

In a smart grid system, as in any system, input will request processing from various sources constantly. This input must be handled properly to avoid catastrophic consequences. Invalid operations or arbitrary execution of malicious code can be devastating. Even improper handling of valid and safe input or code can cause unexpected results. Many of these vulnerabilities including most Structured Query Language (SQL) injection and a significant number of cross-site scripting vulnerabilities can be prevented with sufficient input validation [68]. The objective of most of these attacks is to create malformed or specially crafted messages to a specific node or server which contains the targeted vulnerability. From this point, the attacker can make use of a buffer overflow or an unprotected operation which can help them in escalating privileges of their own malicious process. The failure in this situation would be assuming that the data received will be of the expected message format, while instead, once the malformed messages are parsed, exceptions may be caused including arbitrary code execution.

SQL injections are a type of attack that is easy to avoid in most environments, but are vulnerability exceedingly more common now that utilities choose to utilize web-based interfaces. They are still prevalent in today's computing society due to the many avenues of usefulness of the attack in which system administrators leave unsecured, and the type of data stored on targeted servers. These attacks normally exploit web applications or service interfaces by inputting specially crafted SQL queries into available forms belonging to these websites. Vulnerabilities such as incorrectly filtered data or inadequate typing can cause these maliciously crafted statements to be executed [69, 70].

Cross-site scripting (XSS) and cross-site request forgery (XSRF) are also a vulnerability inhabited by many web applications. These vulnerabilities allow the attacker to inject their own malicious scripts into a web site and simply wait for the victim system to visit. JavaScript has been the most prevalent of the scripting used, but it also extends to ActiveX, HTML, Java, VBScript, and Flash scripting [71, 72]. Vulnerable systems normally do not sanitize the results of the HTTP query parameters and process or execute the commands in their malicious state. Also, the permissions granted the sites that the malicious scripts are downloaded from grant these scripts the same elevated rights.

XSRF allows for arbitrary requests to be sent on the victim's behalf. These requests can be maliciously executed by scripting or simply web browsing [73]. These scripts or actions like XSS are granted the permissions of the site from which they are accessed or downloaded from. A simple example would be for a user to browse the web while he/she has a valid online energy services session open. Upon browsing to a specific website which has a XSRF vulnerability and a malicious image posted which references the action of withdrawing money from the victim's banking website. Therefore, these attacks basically use cookies or the authentication previously established to forward requests via the unsuspecting victim.

In some instances, devices interconnected in smart grid networks employ legacy operating systems that are no longer receiving support which introduces vulnerabilities unique to that software. Also, cloud/utility computing introduced into the grid creates vulnerabilities which must be of concern.

False data injections as described in [74] are used to input manipulated measurements of specific state variables from demand-side or supply-side devices on the smart grid network.

Attacks such as these provide state estimation systems with data which will create abnormalities in a power system and may result in the compromise of supervisory or power controlling devices on the grid. Also, these types of load altering attacks modify actual loads at specific locations in order to disturb the balance between supply and demand or to allow the customer to relieve himself of a portion of his power bill. This can be achieved by maliciously modifying one of the following: energy that demand-nodes demand, energy that supply nodes can supply, and states of the energy links.

Manipulation of data sources in communication with systems in the grid, especially SCADA systems, can cause them to change state in accordance with the data relayed. In an environment which automation is prevalent and necessary, automatic operation based on data input should be assured. This type of action can lead to special case vulnerability for an attacker.

4.2.6 Other Attacks

One such attack which exploits availability is network barge-in [72]. This type of threat can be executed by masquerading or piggybacking open connections such as Wi-Fi in these networks. In the Home Area Network (HAN) or Neighborhood Area Network (NAN), specific devices communicate with each other to relay energy usage information. A malicious attacker can gain access to the network and piggyback on the connection which is established between a smart appliance and a smart meter or aggregation point. With input of malicious or misleading data, the smart appliance may falsify data or be taken over completely, not only risking secure authentication data of the user, but giving the attacker a valid entry point into the grid networks.

A man-in-the-middle attack is also an option for an attacker in this environment. With access to a HAN or NAN in the smart grid, the attacker can intercept communications and relay with or without modifying its contents.

As has been analyzed, there are many vulnerabilities present in the grid. With this in mind, a list of possible attacks to mechanisms that may be vulnerable is listed below in Table 4.

Table 4: methods to exploit software vulnerability. Hardware employing software with specific vulnerability may include: SCADA, HMI, PMU, AMI, Protective Relays, PLC, IED.

Attack Type	Description	Devices Affected	Defense
Buffer Overflow [23]	An operation which writes data and overwrites adjacent memory.	Devices employing software vulnerable to write exploitation (Networked Devices)*	Bound checking, safe coding procedures, ASLR
Race Cond [63]	Programming flaw in which the result of the output is dependent on sequence of events.	Devices employing software with improper input validation and Quality of Service (QoS)*	Increase integrity checks, strategic checkpoints
SQL Injection[63,75]	Submitting malicious SQL statements in a web form to a SQL database.	Databases	Query sanitization (based on DB)
Cross-site Scripting [72, 76]	Injection of client-side script into web pages exploiting web browsers or web applications.	Servers using scripting languages	Disallowing untrusted data in HTML pages, Sanitization,
Cross-site Request Forgery [71, 73]	A session hijacking technique in which a hacker masquerades as a trusted user.	Servers using scripting languages	Cookie Security, Authenticate per request, “NoScript” declaration
OS Injection	Executing commands via a web interface on a remote server.	Devices employing software vulnerable to injection	Proper coding practices
DoS [77, 78, 79, 80, 81]	Utilizing machine resources or making resources unavailable for other users	Devices Providing resources: SCADA, EMS, AMI, PLC	QoS, Distributed Servers, ACLs
Phishing [82,83,84]	Using methods to masquerade as a trusted party to gain information from a user.	Devices operated by users	Web Browser Extensions, Training Programs
Malicious Rem Media [2]	Devices containing malicious software	Devices operated by users	Employee Training Programs
Backdoor Admin Cred[42]	Unauthorized user using admin credentials to gain access to hardware.	Mainly SCADA	Vendor selection, Access controls
Fuzzing [82]	Inputting data to a remote networked entity which is monitored for undefined results.	Networked devices serving as servers: HMI	Address Randomization, Stack protection, buffer length checking
Crypto Key Flash Extraction [36, 85, 86]	Accessing device hardware directly with specific tools to extract data	AMI	Physical Protection, Data Encryption
Flash Image Manipulation [36, 85, 86]	Modifying software images before installment	AMI	Physical Protection, Data Encryption
Meter Bypass [36, 85, 86]	Masquerading or hijacking a communication session stream	AMI	Physical Protection, Data Encryption, Authentication
Meter Measurement Modification [36, 85, 86]	Modifying AMI to report incorrect measurements	AMI	Physical Protection
Extract RAM [36, 85, 86]	Accessing the device hardware directly with specific tools to extract RAM.	AMI	Physical Protection, Data Encryption
Extract Firmware [63]	Accessing the device hardware directly with specific tools to extract firmware in memory.	AMI	Physical Protection, Data Encryption, Update Signing
Watering Hole [87]	Injecting malicious code into a web page which a target victim is likely to visit	Devices operated by users	Web Browser Extensions, Training Programs
False Data Injection [40, 88]	Manipulating power systems states or readings by injecting false load data via AMI/sensors	SCADA, PMU, Transformers, AMI, EMS	Temporal/Spatial-based anomaly detection, Sensor Protection
Spoofing [61]	Adding an end system to the grid network and falsely using a legitimate identity	AMI	Integrity Checking, Physical deterrent,
Worms/Malware	Executing malicious or self-propagating software on the grid network	Potentially all devices*	IDS, IPS, AV

5. Countermeasures

Countermeasures are imperative in today's integrated infrastructure as IP is commonly used to simplify integration of the many parts of the grid and makes communication more standardized. Any successful set of countermeasures or complete security system needs to have multiple defensive mechanisms and multiple detection points. Current security mechanisms such as firewall, anti-virus, and intrusion detection systems should be employed in smart grid systems, as they have defined and useful purposes. Also, new security mechanisms, such as PMUs should be implemented here. The paper [89] presents three key services that need to be in place to have a secure smart grid system: prevention, detection, and response.

Prevention in a secured infrastructure should be composed of access control authentication in order to prevent unauthorized access. Detection should serve the purpose of flagging specified actions or signatures and monitoring the system as a whole. Response should include signature forensics, decision analysis, and contingency procedures [89].

Physical security should include several measures which include considerations in these areas [90]: electronic access control, response to emergency situations, video surveillance and monitoring, geographical location, and tamper detection and reporting.

Access control in a smart grid environment serves the same purpose of strict and specific authorization as in any other cyber network or physical premises. Access control in this setting should build upon currently available technologies and also define relationships between entities and authorized domains in a manner which they can be identified across multiple domains, while assuring real-time access [50].

Well-rehearsed policy should be in place in order to avoid incidents from escalating from small to detrimental. Employee training and sensing devices can assure this. Monitoring and logging equipment should be implemented in any secure infrastructure, with routine evaluation and response actions.

In addition to these, more sophisticated and likely expensive measure can be taken, such as burying distribution equipment underground, enhancing security technology to create a more robust physical infrastructure, or a physical location which is less vulnerable to attack or incident. Hiring personnel to guard the premises of critical infrastructure is instrumental in fortifying physical defense. Tamper proofing field devices and implementing protocols such as invalidating keys when evidence of tampering on is detected should also be implemented on these smart grid systems [91].

The papers [77, 78, 79] detail DoS and DDoS attacks. DoS security mechanisms include preventive methods which will allow a victim to endure the attack or remove the attack vector altogether. This can involve a type of QoS identification or a access control which only lets specific users access to necessary resources [40, 77]. The difficulty of finding a solution to DDoS attacks is that a most effective method is distributed. This means that there must be a coordinated response in place which will be deployed from many different points on the internet [67]. The first and least likely of solutions would be to make arbitrary systems secure from outward attack. This would reduce the ability of an attacker to create a botnet [92], and effectively remove the distributed attack surface of the malicious individual. Another method of prevention is to avoid protocol functions that are expensive for server entities and cheap for the client which are frequently used for DoS attacks [67]. This can be handled by assuring that resources are committed to a client only after proper authentication [93], utilization of proxy servers with sufficient resources [77], protocol scrubbing (to remove protocol uncertainties which can be misused for attacks) [94], and methods to detect spoofing downstream which utilized outside sources such as ISPs of governmental services.

An approach in which resources are served from a distributed architecture may also mitigate DoS attacks [95]. This allows service to be re-routed in the case of failure at a specific location on a network instead of incurring a loss of connectivity. The paper [94] proposes a solution based on data fusion. Where local detection techniques are employed and data is relayed to aggregation points where it is analyzed and action is designated. The number of nodes involved in the data fusion is determined by the detection sensitivity of an attack or a more traditional method of detection which incorporates all nodes on the network in the data fusion and analysis procedure.

Sufficient network resiliency provided by protocols, standards, and architecture may improve mitigation of such DoS attacks. The various network topology possibilities available all have their shortcomings, and there is no universal solution which removes all threats. Geography and utility preference and capability play a large role in the selection of a service topology. For AMI specifications, a meshed network topology, which is the topology of choice for the smart grid, provides quality resilience, and several other requirements [96]. The paper [97] proposes several requirements which help ensure resiliency in smart grids: AMI functionality, flexibility in DR, management of grid incidents, and asset security (cyber and physical).

The advent of remote metering allows for the utilities or other control entities to read and control electricity delivery and usage at the consumer endpoint. This allows for automatic route modification in case of line disruption to allow for continued delivery in the case of an emergency in a specific location, and even isolation of portions of the network in the instant of malicious intrusion. DR allows for generation to better match the consumption. In better regulating the generation as closely to demand as possible overloading and underproduction can be avoided. This will reduce brownouts and blackouts.

The expected resiliency, when considering its real-time operation, of grid operations can be described as having a certain threshold relative to the latency requirements of the data, and operational requirements of the devices. Therefore, specific measures must be taken to deliver data expected above a lower bound that would disrupt the operation of the grid due to insufficient or incorrect data. These control mechanisms help ensure this attribute.

Race conditions in the smart grid may be deterred by utilizing one or more of several methods. These include multiple checks which distinguish the validity and integrity of the data, while moving the checkpoints closer to the source of origination. Also, immutable binding will provide for exclusive use of resources [51]. There is the possibility of race conditions outside of specific smart grid operational data. Example of this can be seen in race conditions found in widely used universal protocols such as Dynamic Host Configuration Protocol (DHCP). Many race conditions may occur on the software side which is a result of poor programming. Any implementation of protocol or procedure on any network hosted on the smart grid should be secured in such a way that resolves these race conditions appropriately. This may require removing or securing common protocols, or ample testing for software which may contain these types of errors.

SQL injections have been used maliciously in web applications to extract data in an unauthorized manner. Attackers can take advantage of attacking through many potential vulnerabilities (user input, cookies, server variables, etc. [70]), with possibility of revealing or compromising a network in several ways. This type of attack becomes easier as utilities become more reliant on web interfaces to provide consumers with services. These services and interfaces which the utility may host or utilize through an external cloud can create more vulnerabilities. Mitigation techniques include appropriately stripping away characters or strings used in SQL queries that can be used maliciously. This would be a process specific to the DB, allowing only strings relevant to the search [69]. The paper [70] presents several other mitigation techniques: black box testing, penetration testing and monitoring based on known patterns (including static code checking), methods for type correctness checking (including query development paradigms), replacing unregulated query binding to a type-checked API (including IDS and instruction set randomizing), and replaces normal SQL keywords with a randomized set.

Static code checking is very valuable in that the form of SQL queries is known, and limiting queries to a specific standard is essential. For example, strictly limiting a query to a single command, while checking the type of command and the authorization level of the user, can help prevent ambiguous requests. Query development paradigms and instruction set randomizing require the programmer to develop a subset of commands in which the DB engine will qualify as valid. These commands should be limited to the set of valid commands relative to the user's privilege level and remove the ability of unauthorized users to modify records or access data outside of their authorization. An IDS implementation can be used to detect SQL injection via an anomaly-based or signature-based method [98]. An ideal location for this IDS would be in front of the DB in the network in question and would specifically evaluate SQL statements being forwarded to the server. A signature for an IDS in this context can be as simple as a specific query or a sequence of SQL keywords, while an anomaly is anything that creates or is equivalent to abnormal system function [98].

Cross-site scripting can be mitigated in the design of a web page by disallowing untrusted data in specific elements of an HTML document and escaping vulnerable and untrusted texts before allowing them in the body of the document [69, 76]. An HTML policy engine should be used to validate or clean user created HTML in an outbound way [76]. Valid cookie security is imperative as well as script disabling. While these mitigation techniques are executed on the web page side, Cross-site request forgery can be mitigated from the user side by carefully implementing a privacy/security plan which includes avoiding malicious links and cached data presented at login pages. According to [71, 73], the main method of mitigating this attack is to constrain input and encode output. Some areas of concern that can help prevent or eliminate request forgeries are listed below: cookie session life, user specific authentication in order to submit a form, and mechanism to verify request headers on web page redirects.

The paper [71] details the synchronizer token pattern usage which should be implemented in the sensitive operation request process of the user. This process is a mechanism which requires the user to input a token into the HTML form in order for that specific step in the process to be valid. This process is initiated at several different stages in the operation completion process [71]. This token requirement process may utilize any client identification attributes including a type of Personal Identification Number (PIN) and is normally referred to as a challenge token.

A privacy/security plan which trains workstation users on the smart grid network, or corporate networks connected to it to identify phishing attempts helps mitigate multiple types of these attacks, along with browser extensions which disallow phishing efforts [82].

File fuzzing is normally conducted to search for buffer overflow, DoS, SQL injection, Format String bugs etc. This simple method of inputting large amounts of possibly random data into a system or network can greatly benefit programmers and administrators in finding errors that may be overlooked. Stack protection and buffer length checking are also novel tools [82].

Bad data is detected and identified after the estimation process by the analyzing measurement residuals. False injection attacks can be detected through either spatial or temporal-based methods. Unobservable attacks cannot be expected to always originate from physical locations in close proximity. Therefore, methods should be designed to detect large unobservable attacks which occur and modify loads in a much faster or abnormal rate [70]. Also, protective measures should be taken in order to secure the sensing mechanisms to mitigate these attacks [74, 88].

In protecting against false data, is important to consider preventative and reactive approaches. Firstly, pricing and command signals should be protected using authorized encryption techniques. A sufficient public or private key encryption algorithm together with an authentication mechanism should protect integrity and confidentiality. Also, protection of AMI devices such as the smart meter is integral. Once a malicious individual gains access to a single smart meter, they have the platform to legitimately introduce false values into the grid.

Unobservable coordinated injection attacks can be detected by placing PMUs in strategic positions along a specific bus which will calculate voltage and phase details along that bus [70]. This PMU measurement data can be submitted over the NaspiNet which implements more techniques for secure transmission of data than standard networks, therefore less subject to attacks [67]. Analyzing PMU data as a security technique uses an anomaly-based algorithm which learns the normal load of a specific portion of the network and alerts the correct authority upon deviation. This also alerts command of the exact perpetrator whose load is compromised.

Confidentiality in the grid is a very important matter as privacy must be ensured for all sensitive data. Traffic analysis takes advantage of the availability of data and infers specific details which will allow the attacker to generalize and develop attacks which may exploit vulnerabilities which are assumed from analyzing this data. NIST announced in 2001 FIPS 197 which is the Advanced Encryption Standard (AES). The paper [35] suggests this standard for use in the smart grid for encryption. Triple DES has also been approved, but unlike AES, the computational strength and method of encryption are estimated to only be secure until around 2030. NIST, along with FERC, also recommends the IEC family of protocols for establishing smart grid interoperability [35, 99]. Several of these protocols are listed below in Table 5.

Table 5: IEC Standards Recommended for the Smart Grid [100]

IEC 61970 & **IEC 61968**: present a Common Information Model (CIM) for data exchanges between devices and networks, while **IEC 61970** is for transmission and **IEC 61968** is for distribution
IEC 61850: provides help for substation automation, communication, and interoperability using a often-used data format.
IEC 60870-6: provides help for information exchanges between control centers.
IEC 62351: is for the cyber security of the communication protocols in the above IEC standards.

Meter security is one of the foremost areas of security research in the smart grid [6-10]. Software/firmware attacks require reliable authentication methods to ensure secure data transfer. Secure boot loaders and cryptographic validation is integral when upgrading software [91]. Security in these devices is more or less a tricky matter as resources are limited in these fairly mobile devices. This means that conventional IDS implementations and computation heavy encryption algorithms should not be utilized on these devices. Physical security measures or tamper-proofing should be enabled on a per device basis to remove the ability of an attacker to physically access the meters memory which may contain consumption data or encryption keys. Serial ports and optical ports must be secured physically and required to have authenticated measures.

To truly evaluate the integrity of a system, evaluating entities must be aware of the recentness of measurements and be able to analyze their results while understanding the context in which they were extracted. In a system of systems as diverse and widely interconnected as a smart grid, measurements and characteristics must be analyzed at a very large scale for various software and devices [95, 101].

6. Publicized Attacks

The most infamous of the malware which targets industrial operating or control equipment is Stuxnet [102]. This worm’s attack vector includes the Windows operating system which was employed on Seimens industrial equipment and software. Several variants of Stuxnet targeted five Iranian organizations [102]. Seimens SCADA systems and PLCs were targeted in these organizations with speculation that the US and Israel played a part in the engineering and distribution of the worm [102, 103].

Very recently, Telvent’s network and accessed project files of a control systems used in the electrical grid were breached by hackers. Attackers installed malicious software in order to access the files via a system which was interconnected with a utility’s corporate network. This system was as an intermediary between legacy devices used on either side of the device [104].

Another type of event which deserves consideration is acts of nature. In recent events, Hurricane Irene blacked out over 4 million customers in the eastern US. Also, in June, 2011, 5 million customer in six states lost power for up to a week. Also, in the summer of 2012, hurricane Sandy caused more than 70 billion dollars in damage [105].

In 2008, Tom Donahue, of the CIA, with no knowledge of the perpetrators, explained that there were several distributed attacks on power equipment in several regions outside of the U.S. These attacks were followed by extortion demands and caused disruptions in services [104].

On a lighter note, On Dec. 29, 2008, an individual hacked into the Ozarks Electric Cooperative Corporation's reporting and outage management system in order to upload a custom voice message stating [112], "All of Ozarks Electric's employees have gone home. Call someone who cares."

2003 hosted the Slammer worm. This malware made its way into a private computer network at Ohio's Davis-Besse nuclear power plant in January and removed monitoring equipment for an estimated five hours [106].

In 2005, the National Nuclear Security Administration computers were hacked in order to steal sensitive information on over 1500 contractors and employees, and went unreported upon initial observation of observation [107].

In Baxley Georgia in 2008, a cyber-threat caused a 48 hour emergency shutdown due to a malware injection attack. An unsigned firmware update was attempted and an attacker uploaded a malicious version of firmware which modified data and caused safety systems to be triggered [108]. Several reports of “watering hole” sites which attempt to infect traffic visiting the site which will allow for an attack from inside the network.

Vendor MacAfee reported that a series of relatively unsophisticated attacks, such as SQL injection, over a term of likely four years by Chinese hacker which stole intellectual property from U.S. energy companies [109]. Several companies were attacked through public facing web sites via cyber methods mixed in with social engineering. Once compromising web servers in the Netherlands for attacks several other countries, malicious software with remote administration tools was uploaded to browse areas such as Active Directory. This operation was labeled Night Dragon [109].

Duqu, discovered in 2011 is a worm with a likeness to Stuxnet, while serving a completely different purpose. This worm recorded keystrokes on remote systems which allowed the hackers to create attacks based on information inferred from the data gathered [109].

7. Conclusion and Future Work

Since the natures of the systems in a smart grid environment are complex and critical to the current state of technology and human well-being, they require quality and sufficient security mechanisms and solutions. This must equate to a holistic approach where all threats and vulnerabilities are considered, including future hazards. In the coming years, standards should be enforced in a manner which will alleviate the responsibility of choosing from the numerous security options on the market that the utilities and device manufacturers. The bulk of the current attacks on the smart grid infrastructure are composed of DoS, traffic analysis, AMI compromise, and higher level application attacks. In this paper some of the past attacks on the grid infrastructure were given along with an overview of current smart grid attacks, which will afford us some insight into securing the grid.

Securing the smart grid will require utilities and all other participating parties to take both short-term and long-term views. Also, utilities and vendors are to begin preparing for a much more standards-based future [72]. These industry standards and protocols should address the necessity for a requirements-based level of consistent and interoperable performance. A report detailed in [110] features a MIT report which explains how a single operational entity is needed manage and regulate grid cybersecurity and response and recovery. This should include all domains and not just the bulk portion of the grid as the FERC and NERC regulate. Finally, a near-future look into smart grid progress will likely yield more functionality in processing and beneficial action on the data accumulated by smart grid AMI and sensing processes.

Future research on grid security will encompass IEDs and processes in the customer domain and their vulnerabilities. This domain is the most vulnerable to attack due to customer defined specifications and unregulated operations. HAN’s are normally more easily compromised due to the lack of cybersecurity knowledge of most customers and the interfaces with other devices and networks in the grid. While most devices in this domain should have security mechanisms in place, they are often not enough to mitigate many attacks from prototypical hackers, as vendors have to weigh financial responsibilities against a standards-based evaluation of their product. This effort will also cover security mechanisms for resource lacking devices such as customer IEDs and AMI. With security currently in place, it is difficult to detect malware and certain malicious actions. The paper [111] mentions Trusted Platform Module (TPM) use in devices such as smart meters for authentication purposes, and discusses its cost will likely keep it from being implemented in widespread practical applications.

Furthermore, since the smart grid is not there yet, understanding the attacks and corresponding countermeasures still quite preliminary. Therefore, in our future work, we plan to propose novel attacks to smart grid and to propose corresponding countermeasures.

Acknowledgements.

This work was supported in part by The National Natural Science Foundation of China (NSFC) under grant # 61374200, and the US National Science Foundation (NSF) under grants CNS-0716211, CNS-0737325, CCF-0829827, and CNS-1059265.

References

[1] Farhangi, H.; “The path of the smart grid,” IEEE Power and Energy Mag., vol. 8, pp. 18-28, 2010.

[2] National Institute of Standards and Technology. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 [online] Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

[3] Stefanov, A.; Chen-Ching Liu, "Cyber-power system security in a smart grid environment," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES , vol., no., pp.1-3, 16-20 Jan. 2012.

[4] Amin, S. M.; B. F. Wollenberg; "Toward a smart grid: power delivery for the 21st century," IEEE Power and Energy Mag., vol.3, no.5, pp. 34-41, Sept.-Oct. 2005.

[5] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A Survey of Communication/Networking in Smart Grids," (Elsevier) Future Generation Computer Systems, Vol. 28, No. 2, Feb. 2012, pp. 391–404.

[6] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys & Tutorials, Vol. 14, NO. 4, pp. 981 - 997, Fourth Quarter 2012.

[7] J. Liu, Y. Xiao, and J. Gao, "Achieving Accountability in Smart Grids," IEEE Systems Journal, Vol. 8, No. 2, Jun. 2014, pp. 493-508.

[8] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang, and C. L. P. Chen, "SCADA Communication and Security Issues," (Wiley Journal of) Security and Communication Networks, Vol. 7, No. 1, pp. 175–194, Jan. 2014.

[9] Z. Xiao, Y. Xiao, and D. Du, "Non-repudiation in Neighborhood Area Networks for Smart Grid," IEEE Communications Magazine, Vol. 51, No. 1, pp. 18-26, Jan. 2013.

[10] Z. Xiao, Y. Xiao, and D. Du, "Exploring Malicious Meter Inspection in Neighborhood Area Smart Grids," IEEE Transactions on Smart Grid, Vol. 4, No. 1, Mar. 2013, pp. 214-226.

[11] Y. Xiao, "Editorial," International Journal of Security and Networks, Vol. 6, No.1, pp. 1 - 1, 2011.

[12] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, K.L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," International Journal of Security and Networks, Vol. 6, No.1, pp. 2 - 13, 2011.

[13] Khurana H.; et al., "Smart-Grid Security Issues," Security & Privacy, IEEE, vol. 8, pp. 81-85,2010.

[14] G. Kalogridis, S.Z. Denic, T. Lewis, R. Cepeda, "Privacy protection system and metrics for hiding electrical events," International Journal of Security and Networks, Vol. 6, No.1, pp. 14 - 27, 2011.

[15] Wang J.; Rong, L.; "Cascade-based attack vulnerability on the us power grid," Safety Sci., vol. 47, no. 10, pp. 1332–1336, Dec. 2009.

[16] Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D.; "A Survey on Cyber Security for Smart Grid Communications," Communications Surveys & Tutorials, IEEE , vol.PP, no.99, pp.1-13, 0.

[17] Mihui K; "A survey on guaranteeing availability in smart grid communications," Advanced Communication Technology (ICACT), 2012 14th International Conference on , vol., no., pp.314-317, 19-22 Feb. 2012.

[18] Li, X; Liang, X.; Lu R.; Shen, X.; Lin, X.; Zhu, H.; "Securing smart grid: cyber attacks, countermeasures, and challenges," Communications Magazine, IEEE , vol.50, no.8, pp.38-45, August 2012.

[19] Gungor, V. C.; Lambert F. C.; "A survey on communication networks for electric system automation" Computer Networks, vol. 50, pp. 877-897, 2006.

[20] Kanabar, M.G.; Voloh, I.; McGinn, D.; "A review of smart grid standards for protection, control, and monitoring applications," Protective Relay Engineers, 2012 65th Annual Conference for , vol., no., pp.281-289, 2-5 April 2012

[21] Ayers, L.M.; "Implementing Smart Grid standards: A letter from the trenches," Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES , vol., no., pp.1-5, 13-16 Nov. 2011.

[22] Nano Markets. "Smart Grid Sensing, Monitoring and Control Systems : Market Opportunites 2011" Mar 2011.

[23] SAP Community Network. [Online]. Available: http://scn.sap.com/community/research/blog/2012/08/08/es-in-web-applications-through-automated-type-analysis.

[24] J. Lin, B. Zhu, P. Zeng, W. Liang, H. Yu, and Y. Xiao, "Monitoring Power Transmission Lines Using a Wireless Sensor Network," Wireless Communications and Mobile Computing (WCMC) Journal, John Wiley & Sons, accepted.

[25] L. Wang and Y. Xiao, "A Survey of Energy-Efficient Scheduling Mechanisms in Sensor Networks," ACM/Springer Mobile Networks and Applications (MONET), Vol. 11, No. 5, 2006, pp. 723-740.

[26] Flick, T.; Morehouse J.; "Securing the Smart Grid" Syngress Pub. Sept 23, 2010. pp23.

[27] North American Reliability Corporation. "Reliability Standards" [Online]. Available: http://www.nerc.com/page.php?cid=2|20.

[28] Amin M.; (EPRI) Security Challenges for the electricity infrastructure. IEEE Computer (Security and Privacy Supplement) Volume 24, Number 4, pp 8-10. April 2002.

[29] F. Li, B. Luo, P. Liu, "Secure and privacy-preserving information aggregation for smart grids," International Journal of Security and Networks, Vol. 6, No.1, pp. 28 - 39 , 2011.

[30] J. Zhang, C. A. Gunter, "Application-aware secure multicast for power grid communications," International Journal of Security and Networks, Vol. 6, No.1, pp. 40 - 52 , 2011.

[31] Association of Home Appliance Manufacturers. "Assessment of Communications Standards for Smart Appliances". [Online] Available: http://www.aham.org/ht/a/GetDocumentAction/i/50696.

[32] National Communications System, "Supervisory control and data acquisition (SCADA) systems," Technical Report, Oct. 2004, available at: http://www.ncs.gov/library/tech bulletins/2004/tib 04-1.pdf

[33] IEC TC57, "Power system control & associated communications - data & communication security," IEC 62351 Part 1 to 8, Technical Specification and Draft, 2010.

[34] Benoit J.; "An Introduction to Cryptography as Applied to the Smart Grid" Cooper Power Systems.

[35] The National Energy Technology Laboratory for the U.S. Department of Energy. "Advanced Metering Infrastructure". February 2008.

[36] Kanabar, M.G.; Voloh, I.; McGinn, D.; "Reviewing smart grid standards for protection, control, and monitoring applications," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES , vol., no., pp.1-8, 16-20 Jan. 2012.

[37] Giani, A.; Bitar, E.; Garcia, M.; McQueen, M.; Khargonekar, P.; Poolla, K.; , "Smart grid data integrity attacks: characterizations and countermeasuresπ," Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on , vol., no., pp.232-237, 17-20 Oct. 2011.

[38] Dan, G.; Sandberg, H.; "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," Proceedings of the IEEE SmartGridComm , Oct. 2010.

[39] Biba, K. J.; "Integrity considerations for secure computer systems," Technical report, MITRE Corp., Apr, 1977.

[40] Zheng, Y. L.; Leiwo, J.; “A Method to Implement a Denial of Service Protection Base”. In Information Security and Privacy, volume 1270 of LNCS, pages 90{101, 1997.

[41] Danezis, G.; Clayton, R.; “Introducing traffic analysis”. In Digital Privacy: Theory, Technologies, and Practices, Chapter 5. Auerbach Publications, 2008.

[42] Schwars, K.; “NIST recommends IEC 61850 and other IEC TC 57 Standards for Regulation” [Online] Available: http://blog.iec61850.com/2010/10/nist-recommends-iec-61850-and-other-iec.html.

[43] Datta Ray, P.; Harnoor, R.; Hentea, M.; , "Smart power grid security: A unified risk management approach," Security Technology (ICCST), 2010 IEEE International Carnahan Conference on , vol., no., pp.276-285, 5-8 Oct. 2010.

[44] ABB Inc. Security in the Smart Grid. ABB White Paper.Available: http://www02.abb.com/db/db0003/db002`8.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_Security+in+the+Smart+Grid+%28Sept+09%29_docnum.pdf

[45] Meliopoulos, S.; Cokkinides, G.; Huang, R.; Farantatos, E.; Sungyun Choi; Yonghee Lee; Xuebei Yu; , "Smart Grid Infrastructure for Distribution Systems and Applications," System Sciences (HICSS), 2011 44th Hawaii International Conference on , vol., no., pp.1-11, 4-7 Jan. 2011.

[46] Wei, D.; Lu, Y.; Jafari, M.; “On protecting industrial automation and control systems against electronic attacks,” in Proc. IEEE Int. Conf. Autom. Sci. Eng., Sep. 2007, pp. 176–181.

[47] Z. Xiao, B. Fu, Y. Xiao, C. L. P. Chen, and W. Liang, "A Review of GENI Authentication and Access Control Mechanisms," International Journal of Security and Networks (IJSN), Vol. 8, No. 1, 2013, pp. 40-60.

[48] J. Liu, Y. Xiao, and C. L. P. Chen, "Internet of Things’ Authentication and Access Control," International Journal of Security and Networks (IJSN), Vol. 7, No. 4, 2012, pp. 228-241. DOI: 10.1504/IJSN.2012.053461

[49] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and Access Control in the Internet of Things," the proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW 2012), pp. 588-592.

[50] Cheung, H.; Hamlyn, A.; Mander, T.; Cungang Yang; Cheung, R.; , "Strategy and Role-based Model of Security Access Control for Smart Grids Computer Networks," Electrical Power Conference, 2007. EPC 2007. IEEE Canada , vol., no., pp.423-428, 25-26 Oct. 2007

[51] Amin M.; Wollenberg, B.F.; “Toward a smart grid: power delivery for the 21st century,” IEEE Power and Energy Magazine, Vol.3, No. 5 Sept.-Oct. 2005, pp. 34-41.

[52] Seshadri, A.; Luk, M.; Shi, E.; Perrig, A.; van Doorn L.; Khosla, P.; “Pioneer: Verifying integrity and guaranteeing execution of code on legacy platforms,” In ACM Symposium on Operating Systems Principles, pp. 1-15, Oct. 2005.

[53] Cheung, H.; Hamlyn, A.; Mander, T.; Cungang Yang; Cheung, R.; , "Role-based model security access control for smart power-grids computer networks," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE , vol., no., pp.1-7, 20-24 July 2008

[54] Chen, X., Sung Kim, H.; “RBAC for Home Area Network based Smart Grid” Journal of the Korea Institute of Information Technology Convergence, Vol. 3, No. 2, pp. 95-101, 2010.

[55] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A Survey of Key Management Schemes in Wireless Sensor Networks," Computer communications Journal, Vol. 30 No. 11-12, Sep. 2007. pp. 2314–2341.

[56] Zetter, K.; “SCADA System’s Hard-Coded Password Circulated Online for Years”. [Online] Available: http://www.wired.com/threatlevel/2010/07/siemens-scada/.

[57] P. Rus. “SCADA vulnerabilities now with hardcoded backdoors” [Online] Available: http://www.serverbeheersupport.nl/2012/04/scada-vulnerabilities-now-with-hardcoded-backdoors/.

[58] Metke, A. R.; Ekl, A. R.; “Security Technology for Smart Grid Networks,” IEEE Transactionson Smart Grid, vol. 1, 2010.

[59] Smith, S.W.; "Cryptographic scalability challenges in the smart grid (extended abstract)," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES , vol., no., pp.1-3, 16-20 Jan. 2012.

[60] Nabeel, M..; Zage, J.; Kerr, S.; Bertino, E.; Kulatunga, N.; “Cryptographic Key Management for Smart Power Grids 2012-1”

[61] Nagaratna, M.; Prasad, V.K.; Kumar, S.T.; "Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking Based Detection and Filtering (EMDAF)," Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference on, vol., no., pp.753-755, 27-28 Oct. 2009.

[62] Jiang, M.; Hu, M.; Zhou, J.; Peng T.; "Design and Implementation of IP-SAN Based on Third Party Transfer Protocols," Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium on , vol.1, no., pp.188-192, 3-4 Aug. 2008.

[63] Ernest Young. “Attacking the Smart Grid” Available: http://www.ey.com/Publication/vwLUAssets/Attacking_the_smart_grid/$FILE/Attacking-the-smart-grid_AU1058.pdf. December 2011.

[64] Katzir, L.; Schwartzman, I.; , "Secure firmware updates for smart grid Devices," Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on , vol., no., pp.1-5, 5-7 Dec. 2011

[65] Divan, D.; Johal, H.; “A Smarter Grid for Improving System Reliability and Asset Utilization,” Power Electronics and Motion Control Conference, August, 2006.

[66] Brown, R.E.; , "Impact of Smart Grid on distribution system design," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE , vol., no., pp.1-4, 20-24 July 2008.

[67] Mirkovic, H.; Reiher, P.; “A taxonomy of DDoS attack and DDoS defense mechanisms,” SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39C53, 2004.

[68] van Vliet, M; Yearsley, J.; Ludwig, F.; Vögele, S.; Lettenmaier, D.; Kabat, P.; “Vulnerability of US and European electricity supply to climate change”. Nature Climate Change , (2012).

[69] The Open Web Application Security Project [Online]. Available: https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet.

[70] Halfond, W. G.; Vegas, J.; Orso, A.; “A Classification of SQL Injection Attacks and Countermeasures”, in Proc. Of the Intl. Symposium on Secure Software Engineering, Mar 2006.

[71] "Cross-Site Request Forgery (CSRF)". OWASP, The Open Web Application Security Project. 4 September, 2012.

[72] Chasko, S.; LaPorte, T.J.; “Smart Grid Security: Preparing for the Standards-Based Future” [Online]. Available: http://www.befutureready.com/security/Landis-and-Gyr-Smart-Grid-Security.pdf.

[73] Chou, N.; Ledesma, R.; Teraguchi, Y.; Boneh, D.; Mitchell. J.; “Clientside defense against web-based identity theft”. In Proc. 11th Annual Network and Distributed System Security Symposium (NDSS ’04), February 2004.

[74] Zheng, Y. L.; Leiwo, J.; “A Method to Implement a Denial of Service Protection Base”. In Information Security and Privacy, volume 1270 of LNCS, pages 90{101, 1997.

[75] Energy Transmission in the United State. [Online} Available: teeic.anl.gov/er/transmission/restech/dist/index.cfm.

[76] Shiflett, C.; "Security Corner: Cross-Site Request Forgeries". php|architect (via shiflett.org). (December 13, 2004).

[77] Schuba, C. L.; Krsul, I. V.; Kuhn, M. G. ; Spafford, E. H. ; Sundaram, A.; Zamboni, D.; “Analysis of a denial of service attack on tcp,” in Proc.

[78] Yaar, A.; Perrig, A.; Song, D.; “Pi: A path identification mechanism to defend against DDoS attacks,” in Proc. IEEE Symposium on Security.

[79] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39C53, 2004.

[80] B. Sun, F. Yu, K. Wu, Y. Xiao, V. C. M. Leung, "Enhancing Security using Mobility-Based Anomaly Detection in Cellular Mobile Networks," IEEE Transactions on Vehicular Technology, Vol. 55, No. 4, July 2006, pp.1385-1396.

[81] B. Sun, Y. Xiao, and R. Wang, "Detection of Fraudulent Usage in Wireless Networks," IEEE Transactions on Vehicular Technology, Vol. 56, No.6, Nov. 2007, pp. 3912 - 3923.

[82] Godefroid, P.; Levin, M.; Molnar, D.; “SAGE: Whitebox Fuzzing for Security Testing”. Queue, v.10 n.1, January 2012.

[83] Y. Xiao, C.-C. Li, M. Lei, and S. V. Vrbsky, "Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users from Password Theft," IEEE Systems Journal, Vol. 8, No. 2, Jun. 2014, pp. 406-416.

[84] .M. Lei, Y. Xiao, S. V. Vrbsky, and C.-C. Li, “Virtual Password Using Random Linear Functions for On-line Services, ATMs, and Pervasive Computing," Computer Communications Journal, Elsevier, Vol. 31, No. 18, Dec. 2008, pp. 4367-4375.

[85] European Network and Security Information Agency. “Smart Grid Security”. [Online] Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

[86] C4 Security.; “The Dark Side of Smart Grid – Smart Meters (in) Security” available: www.c4-security.com/The Dark Side of the Smart Grid - Smart Meters (in)Security.pdf.

[87] K. Spett. SPI Dynamice “Are your web applications vulnerable”. 2005. Available: http:// http://www.gwtis.com/whitepapers/sqlinjectionwp.pdf

[88] Bhattarai, S.; Ge, L.; Yu, W.; “A Novel Architecture against False Data Injection Attacks in Smart Grid”, Proceeding of IEEE ICC 2012 – Communication and Information Systems Security Symposium, June 2012.

[89] Ray, P.; Harnoor, R.; Hentea, M.; "Smart power grid security: A unified risk management approach," Security Technology (ICCST), 2010 IEEE International Carnahan Conference on , vol., no., pp.276-285, 5-8 Oct. 2010.

[90] Cisco Systems Inc. “Security for the Smart Grid”, Whitepaper 2009. Available: https://www.cisco.com/web/strategy/docs/energy/white_paper_c11_539161.pdf

[91] Hongkai, L.; Chenghong, X.; Jinghui, S.; Yuexi, Y.; "Green power generation technology for distributed power supply," Electricity Distribution, 2008. CICED 2008. China International Conference on , vol., no., pp.1-4, 10-13 Dec. 2008

[92] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and, J. Zhang, "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures," EURASIP Journal on Wireless Communications and Networking, Volume 2009, Article ID 692654, 11 pages, doi:10.1155/2009/692654

[93] Leiwo, J.; Nikander, P.; Aura. T.; “Towards network denial of service resistant protocols”. In Proceedings of the 15th International Information Security Conference, August 2000.

[94] Malan, G. R.; Watson, D.; Jahanian, F.; Howell. P.; “Transport and Application Protocol Scrubbing:. In Proceedings of INFOCOM 2000, pages 1381{1390, 2000.

[95] Smith P.; et al.; “Network Resilience: A Systematic Approach,” IEEE Commun. Mag., vol. 49, no. 7, July 2011, pp. 88–97

[96] Leon, G.; “Smart Planning for Smart Grid AMI Mesh Networks”. EDX Wireless, LLC. Available: http://www.edx.com/resources/documents/EDX_WP_Smart_Grid_AMI_Mesh_Networks_May_11.pdf

[97] AlMajali. A.; Viswanathan, A.; Neuman. C.; “Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack”. USC/Information Sciences Institute.

[98] Rietta, F.; “Application layer intrusion detection for SQL injection”. In: 44th annual Southeast regional conference, ACM, New York, USA, pp.531-536, 2006.

[99] Wei, D.; Lu, Y.; Jafari, M.; Skare, P.M.; Rohde, K.; , "Protecting Smart Grid Automation Systems Against Cyberattacks," Smart Grid, IEEE Transactions on , vol.2, no.4, pp.782-795, Dec. 2011.

[100] Schwars. K.; “NIST recommends IEC 61850 and other IEC TC 57 Standards for Regulation” [Online] Available: http://blog.iec61850.com/2010/10/nist-recommends-iec-61850-and-other-iec.html.

[101] Seshadri, A.; Luk, M.; Shi, E.; Perrig, A.; van Doorn, L.; Khosla, P.; “Pioneer: Verifying integrity and guaranteeing execution of code on legacy platforms,” In ACM Symposium on Operating Systems Principles, pp. 1-15, Oct. 2005.

[102] Cherry, S.; Constantine, L.; "Sons of Stuxnet". IEEE Spectrum. (14 December 2011).

[103] Markoff, J.; "Malware Aimed at Iran Hit Five Sites, Report Says" . New York Times. p. 15. (11 February 2011).

[104] Krebs, B.; “Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent” [Online].Available: http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

[105] Gonsalves, A.; “Damage from attack on power grid would surpass Sandy”. [Online] Available: http://www.networkworld.com/news/2012/112912-damage-from-attack-on-power-264620.html. November 29, 2012.

[106] Poulson, K.; "Slammer worm crashed Ohio nuke plant network." SecurityFocus. Aug 19, 2003. (accessed Nov 27, 2009).

[107] Hebert, J.; Associated Press. “DOE Computers Hacked; Info on 1,500 Taken” [Online] Available: http://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=132x2673379

[108] Krebs. B.; Cyber Incident Blamed for Nuclear Power Plant Shutdown [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html. (2008, Jun.)

[109] McAfee Foundstone Professional Services and McAfee Labs “Global Energy Cyberattacks: “Night Dragon”. 10 February 2010

[110] D. Perera. Fierce Homeland Security. “MIT: Cyber attack on electric grid ‘almost certain’” December 2011 [Online] Available: http://www.fiercehomelandsecurity.com/story/mit-cyber-attack-electric-grid-almost-certain/2011-12-05.

[111] Tabrizi, F.M.; Pattabiraman, K.; "A model for security analysis of smart meters," Dependable Systems and Networks Workshops (DSN-W), 2012 IEEE/IFIP 42nd International Conference on , vol., no., pp.1-6, 25-28 June 2012.

[112] http://www.networkworld.com/article/2217684/data-center/attacks-on-power-systems--hackers--malware.html