AMI SECURITY ISSUES AND BEST PRACTICES

Aditi Dave
B.E., Gujarat University, India, 2007

PROJECT

Submitted in partial satisfaction of
the requirements for the degree of

MASTER OF SCIENCE

in

SOFTWARE ENGINEERING

at

CALIFORNIA STATE UNIVERSITY, SACRAMENTO

SPRING
2011
Student:  Aditi Dave

I certify that these students have met the requirements for format contained in the University format manual, and that this Project is suitable for shelving in the Library and credit is to be awarded for the Project.

Dr. Nikrouz Faroughi, Graduate Coordinator

Department of Computer Science
Abstract

of

AMI SECURITY ISSUES AND BEST PRACTICES

by

Aditi Dave

This report discusses about potential Advance Metering Infrastructure (AMI) security threats and best practices to mitigate the risks caused by the security threats. Issues specifically addressed in this report are threats, vulnerabilities and risks. Best practices discussed in the report cover various aspects of security such as: data integrity, accountability, availability and confidentiality.

This project covers the following areas:

First, identify the potential issues affecting the confidentiality, integrity, and availability of information flow in the Advance Metering Infrastructure (AMI). For instance, hacker/terrorist use of malicious software to perform denial of service attacks on AMI.

Second, group the potential security issues with respect to the security concepts: confidentiality, integrity, and availability. Third, investigate information security best practice(s), which may apply to Advance Metering Infrastructure against the security threats. Best practices such as use of firewalls for perimeter defense, intrusion detection, incident response handing, defense in depth, etc are well known in the information
security area. These best practices are intended to mitigate actions that violate confidentiality, integrity, and availability of the information flow.

______________________, Committee Chair
Dr. Isaac Ghansah

______________________
Date
DEDICATION

This project is dedicated to my beloved parents Jagdishchandra P Dave, Neela Dave and my brother Ankit Dave for their never-ending sacrifice, love, support and understanding.
ACKNOWLEDGEMENTS

I would like to extend my gratitude to my project advisor Dr. Isaac Ghansah, Professor, Computer Science and Engineering for guiding me throughout this project and helping me in completing this project successfully. I am also thankful to Dr. Scott Gordon, Professor, Computer Science and Engineering, for reviewing my report. I am grateful to Dr. Nikrouz Faroughi, Graduate Coordinator, Department of Computer Science, for reviewing my report and providing valuable feedbacks. In addition, I would like to thank The Department of Computer Science at California State University for extending this opportunity for me to pursue this program and guiding me all the way to become a successful student.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedication</td>
<td>vi</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>vii</td>
</tr>
<tr>
<td>List of Figures</td>
<td>xi</td>
</tr>
<tr>
<td>List of Abbreviations</td>
<td>xii</td>
</tr>
<tr>
<td>1. INTRODUCTION TO SMART GRID</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Introduction to Electric Grid and it’s Drawbacks</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Smart Grid as a Solution to Electric Grid</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Need for Smart Grid Security Research</td>
<td>2</td>
</tr>
<tr>
<td>1.4 Smart Grid Overview</td>
<td>3</td>
</tr>
<tr>
<td>2. ADVANCED METERING INFRASTRUCTURE (AMI)</td>
<td>10</td>
</tr>
<tr>
<td>2.1 AMI Components</td>
<td>10</td>
</tr>
<tr>
<td>3. AMI SECURITY THREATS</td>
<td>14</td>
</tr>
<tr>
<td>3.1 Listening AMI Communications</td>
<td>14</td>
</tr>
<tr>
<td>3.2 Modification of AMI Data</td>
<td>15</td>
</tr>
<tr>
<td>3.3 Interactions of AMI Components</td>
<td>15</td>
</tr>
<tr>
<td>3.4 Malicious Code Planted in System</td>
<td>16</td>
</tr>
<tr>
<td>3.5 Service Spoofing</td>
<td>16</td>
</tr>
<tr>
<td>3.6 Denial of Service</td>
<td>17</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>3.7 Denial of Action</td>
<td>17</td>
</tr>
<tr>
<td>3.8 Insider Attack</td>
<td>18</td>
</tr>
<tr>
<td>3.9 Unauthorized Access from Customer Side</td>
<td>18</td>
</tr>
<tr>
<td>3.10 Customer Cheating</td>
<td>18</td>
</tr>
<tr>
<td>3.11 Malicious Update/Patches</td>
<td>19</td>
</tr>
<tr>
<td>3.12 Authenticating and Authorizing Maintenance Personnel to SM</td>
<td>20</td>
</tr>
<tr>
<td>4. AMI SECURITY BEST PRACTICES IN GENERAL</td>
<td>21</td>
</tr>
<tr>
<td>4.1 Basic AMI Cryptography Considerations</td>
<td>21</td>
</tr>
<tr>
<td>4.2 Code Signing and Firmware Authentication</td>
<td>22</td>
</tr>
<tr>
<td>4.3 Against Customer Threat</td>
<td>24</td>
</tr>
<tr>
<td>4.4 The Terrorist and Nation-state Threats</td>
<td>24</td>
</tr>
<tr>
<td>4.5 Information Security Policies</td>
<td>25</td>
</tr>
<tr>
<td>4.6 Software Updates and Patches</td>
<td>25</td>
</tr>
<tr>
<td>4.7 Physical Security</td>
<td>26</td>
</tr>
<tr>
<td>4.8 Data Classification and Retention</td>
<td>27</td>
</tr>
<tr>
<td>4.9 Employee Awareness, Training, and Education</td>
<td>28</td>
</tr>
<tr>
<td>4.10 Incident Response</td>
<td>28</td>
</tr>
<tr>
<td>4.11 Password Requirements and Guidelines</td>
<td>29</td>
</tr>
<tr>
<td>4.12 Threat Modeling</td>
<td>29</td>
</tr>
<tr>
<td>5. BEST PRACTICES SPECIFIC TO AREAS OF SECURITY</td>
<td>31</td>
</tr>
<tr>
<td>5.1 Social Engineering</td>
<td>31</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1-1</td>
<td>Smart Grid Network</td>
<td>4</td>
</tr>
<tr>
<td>Figure 1-2</td>
<td>Working of Smart Grid</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2-1</td>
<td>AMI Components</td>
<td>12</td>
</tr>
</tbody>
</table>
Chapter 1

INTRODUCTION TO SMART GRID

1.1 Introduction to Electric Grid and it’s Drawbacks:

Electric grid is one of the biggest engineering inventions of the 20th century. The biggest drawback of the existing electric grid infrastructure is the lack of two-way communication between customer and energy provider. Customers had no control over the utilities or the energy request. There was no way of constantly monitoring the energy usage. The present electric grid has several additional drawbacks: overburdening and load on electric grid can results in blackouts. Further, the electric grid is generated – stored – transmitted and distributed. Thus, the transmission loss is very high. Further, there is no mechanism for returning the unused energy back to the utility. Thus, the present grid has several drawbacks that lead to Smart Grid research.

1.2 Smart Grid as a Solution to Electric Grid:

Smart Grid provides solution to several existing issues of electric grid infrastructure by providing on-time and on-demand energy to the customers. It is widely distributed using latest technologies to provide real-time monitoring of energy usage. The Smart Grid infrastructure delivers electricity from suppliers to consumers using digital technology to save energy, reduce the cost and increase the reliability and transparency. Smart Grid infrastructure provides energy based on energy needs and thus, saving the energy and reducing the cost. User can predefine and monitor energy requirements by sending the
signals and that makes the smart grid infrastructure transparent. Further, customers can get real time pricing of energy usage. That will help the customer to reduce their bills and save energy. SG can be utilized as a way of addressing some of the critical issues such as: global warming and emergency resilience issues by saving the energy.

1.3 Need for Smart Grid Security Research:
Smart-grid can benefit the whole nation in terms of saving the energy, reducing the cost and wastage. Smart Grid involves two-way communication between the service provider and the customer. Underlying structure of Smart Grid involves many network layers and the communication involves use of different network protocols and different component of SG. Most of the communication protocol and SG components have security threats related (chapter 3 discusses detailed description about the different security threats). Further, Smart Grid infrastructure is made of different components (e.g. Home Area network, Demand response, Advance metering infrastructure, Plug-in electric vehicles etc.). These components are vulnerable to security attacks. If the attacker compromises one of the core component e.g. AMI, they may get access to other components and critical information (security attacks in detail are explained in the chapter 3). Thus, the Smart Grid is vulnerable to various cyber-attacks. The attacks can cause serious issues to mission critical systems (e.g. hospitals, national security agency). Due to the severity of consequences, Smart Grid is considered as one of the critical infrastructures. Thus, US government is spending money and resources to find out security issues with Smart grid components and the communication protocol used. Many research institutes are working
to achieve high quality smart grid infrastructure lay out. There are several research papers from NIST, Sandia lab and other individual researchers. The existing work overlooks some of the security concerns. Further, there are not many documents, which specifically pin points the security issues specific to Advance Metering Infrastructure and best practices against the issues. E.g., report by Sandia lab on “Advanced Metering Infrastructure Security Considerations” does not include details on various threats to the AMI. Further documents from “Open Smart Grid” and NIST discusses Smart grid in general. There are very few documents, which focus on each different component in detail.

In this research, we will cover Advance Metering Infrastructure (AMI). The aim of the project is to find different areas of security and vulnerabilities to AMI. In addition to security risks, the research will cover several best practices to mitigate the risks. We will not cover any experiments or readings for Advance metering infrastructure as meters and protocols are not disclosed for security reasons.

1.4 Smart Grid Overview:

A smart grid infrastructure delivers electricity from suppliers to consumers using digital technology to save energy, reduce cost and increase reliability and transparency. Smart Grid infrastructure provides energy based on energy needs and thus saving energy and reducing the cost. It is an infrastructure, which is being utilized as a way of addressing some of the critical issues such as: global warming and emergency resilience issues.
The primary components of Smart Grid are shown in Figure 1-1. Figure 1-2 explains how the Smart Grid components interact with each other.

The above figure 1.1 explains different components of smart grid and their interaction with each other. Customer will send the request for energy usage by sending the signal to energy providers (e.g. Independent service providers etc.) through the intermediate Smart grid components (e.g. smart meters). The information will then pass through the AMI to the metering system. The components that are covered in the process are Smart meters, home area network, Advance metering infrastructure, demand response etc.
Smart Grid has the following characteristics

- Graceful behavior with power disturbance events
- Actively respond to the customer demands
- Resilient against physical and cyber attack
- Optimizing assets and operating efficiently

Figure 1-2 gives an overall idea of interaction between SG components.
The unique characteristics of smart grid stated above are the reasons why cyber security of the smart grid is imperative. The energy generator will generate the energy. Based on the customer request, the energy will be provided by the utilities to the customer. The pricing signals will be sent from the Advance metering infrastructure head-end to the
customer. The energy usage will be recorded in the Smart meters and will be used for billing.

The Smart Grid has many anticipated benefits such as [3]:

- Improves power reliability and quality.
- Optimizes facility utilization and averts construction of back-up (peak load) power plants.
- Enhances capacity and efficiency of existing electric power networks.
- Improves resilience to disruption.
- Enables predictive maintenance and “self-healing” responses to system disturbances.
- Facilitates expanded deployment of renewable energy sources.
- Accommodates distributed power sources.
- Automates maintenance and operation.
- Reduces greenhouse gas emissions by enabling electric vehicles and new power sources.
- Reduces oil consumption by reducing the need for inefficient generation during peak usage periods.
- Improves cyber security.
- Enables transition to plug-in electric vehicles and new energy storage options.
- Increases consumer choice.
To summarize, concept of Smart Grid improves the existing electric grid infrastructure by adding communication (to and from customer and utilities), monitoring (Smart meters, price signals, and AMI authorities), and control (energy consumption requests by users, AMI authorities). Thus, making the electric grid more efficient and powerful. These added features will provide the maximum throughput while reducing the energy wastage and energy cost. It will benefit customers by providing control over energy usage. At the same time, it will help utilities to better utilize energy request especially during peak hours. Further, it will help industrial or businesses to reduce their energy bill considerably. E.g., normally, the business offices operate during 8-5. The administrator can set the energy usage for cooling system/electricity according to work hours (i.e. 8:00 a.m. - 5:00 p.m.). This will save a lot of energy and reduce bills. Further, new technologies such as plug-in electric vehicles can take advantage of Smart Grid by charging the vehicles during the off-peak hours.

Major reason for this cyber security research is because of the complexity of the smart grid components, the importance of the smart grid as a super-critical infrastructure, and the fact that many reports of potential attacks on the grid have been disseminated in the media. This research should help put some these reports in perspective. Smart Grid infrastructure involves several components and protocols for communication such as: Advance Metering Infrastructure, Demand response, Home area Network, Supervisory Control and Data Acquisition system (SCADA) etc. This research will focus on the Advance Metering infrastructure.
Chapter 2 provides information about Advance Metering infrastructure and its components e.g. Smart Meter, AMI communication network, customer gateway etc.
Chapter 2

ADVANCED METERING INFRASTRUCTURE (AMI)

This chapter contains the basics of AMI and its components. Advanced Metering Infrastructure (AMI) refers to systems that helps to collect customer usage data, measures the collected data and finally analyzes it based on the usage from devices such as electricity meters, gas meters, and/or water meters. AMI is composed of hardware, software, communications, customer associated systems and meter data management software. Thus, AMI is one of the critical parts of the Smart Grid infrastructure.

AMI has many advantages to the energy providers and customers. Customer can define their energy usage and can receive energy on-demand basis. Due to Demand Response system, utilities can send information to AMI for the energy usage efficiently and thus saving energy. Further, utilities can send the signals to AMI regarding energy pricing. AMI system is composed of several sub-components and they all communicate with each other.

2.1 AMI Components:

AMI systems are viewed as consisting of the following components:

- Smart Meter – Smart meter captures meter data and information about energy usage data. Energy usage by customers and other related data is stored in smart meters. Smart Meter is one of the critical components of AMI as it can disclose
customer related information. Customer can see their power usage pattern using Smart meters. Further, they can restrict the power usage and save money by monitoring meter data. The Smart meters are also linked with the utilities and billing systems. Thus, the customer can get real time pricing of the energy.

- **AMI Communications Network** – It helps to establish path for data from Smart meters to AMI headend component. It uses different protocols for communication between the Smart meter and headend components.

- **Customer Gateway** – The customer gateway is an interface that connects AMI components, customer systems and appliances within the customer facilities (E.g. home area network). As shown in the figure 2.1, customer gateway provides communication between the Smart meters, Load control devices and home area network.

- **AMI Head End** – It manages the information flow between the Advance Metering Infrastructure and the external systems such as Meter Data Management. The data will be eventually sent to the billing systems for energy usage.

Figure 2-1 shows different AMI component and their interaction with each-other.
AMI has many advantages to customers, utilities, and other entities. Customers can monitor their energy usage and pricing signals on on-time/hourly/daily bases. Thus, reducing the energy usage during the peak hours will save money for the customer. The customer can use the energy wisely by monitoring the usage data in the smart meters. At the same time, due to less energy consumption during peak hours, the utilities will have to deal with less energy load. Thus, it will benefit both the customers and utilities. Industries are higher energy consumers and they can benefit from Smart meters the most.

Figure 2-1: AMI Components [4]
They can set the smart meters according to work-hours/holidays etc and can save lot of energy.

AMI involves customer information and communication with utilities. AMI components communicate with each other via different protocols. Due to the behavior of AMI, it is highly vulnerable to cyber attacks. The attack profile can vary from unethical customers to terrorists. Whenever the AMI will be implemented, security threats to AMI components will increase. Hackers have started to penetrate the weaknesses in the AMI components. Cyber Attacks on AMI will not only effect utilities in terms of legal issues but to the customers, billing systems and nation. Regulatory fines and legal issues can cause damage to utilities. Thus, AMI vendor should establish certain standards for AMI manufactures. The manufactures should adopt security best practices for AMI. They should consider confidentiality, integrity, privacy and high availability as their basic concerns while manufacturing the AMI.

Chapter 3 is about security issues to the Advance metering Infrastructure.
Chapter 3
AMI SECURITY THREATS

This chapter discusses various security threats to AMI. Due to the complexity of the AMI components, it is vulnerable to many security threats. The following types of security threats are possible on AMI of Smart Grid.[5]

3.1 Listening AMI Communications:
Listening AMI communication will affect Confidentiality of transmitted data. Unauthorized person can get access to the communication channel and listen to the communications between customer and utilities or within the AMI. Thus, the unauthorized user can intercept the real-time data transferred between customers and utilities. Further, they can examine the message and can perform traffic analysis to harm both customer and utility. E.g., Customer sends a signal to utilities to shut down the cooling system for 5 days. The listener can easily know that there is nobody at home during the 5 day time period. They can use this information and can steal the house. Hackers can use different listening methods to get access to the communication data e.g. by using electromagnetic /radio frequency to intercept the communication data, social networking. The hacker can change the data coming from either customer/utilities and affect the other greatly.
3.2 Modification of AMI Data:
Once the unauthorized person/hacker has access to the AMI communication data, he/she can modify the data either by changing the data or intercepting the data. Due to the security risk attached, the AMI manufactures should design the AMI to achieve non-repudiation of data. Non-repudiation will benefit both the customer and utilities as customer/utility cannot deny after sending the message to each other.

3.3 Interactions of AMI Components:
Interactions of AMI components with the environment could lead to unauthorized access to AMI communication information and modification of AMI data. Further, it may lead to denial of service to authorized/legitimate users. This can affect confidentiality, integrity, availability and accountability of data. This attack can be performed in many ways:
Masquerade: the attacker acts as an authorized user to gain the access or try to get privilege higher than assigned.
Bypassing Controls: attack the system in such a way to avoid any credential checks.
Physical Intrusion: People may physically intrude into AMI system components like Smart Meter to perform unauthorized actions.
Man-in-the-Middle: The attacker makes independent connections with the victims and relays messages between them. Thus, the customer will believe that they are talking to legitimate party at other end when in fact the communication is controlled by the attacker.
3.4 Malicious Code planted in System:

Malicious code/components planted in the system could lead to unauthorized access to AMI communication information, modification of AMI data and denial of service to authorized users. This can affect confidentiality, integrity, availability and accountability of data. This can be done in several ways:

Virus/Worms: If the attacker can get a way to the system, they can deploy Virus/Worms in the system. Virus is a program that increases its number by copying itself. Worm uses a network to send copies to increase the number and this process is done without user intervention. As AMI communicates between user and utility, if anyone from user/utility is infected by virus/worm, there are higher chances of corrupting the other. E.g. computer A gets a virus. Now A will communicate to other AMI components and the utility. It will effect user B,C etc as they are sharing the same network. This chain will affect all connected users.

Trojan Horse: It’s a type of malware that provides unauthorized access to the system. Once the attacker has access to one system in the AMI network he can deploy the Trojan horse in the system. The infected system will communicate with other components and can affect them during the communication.

3.5 Service Spoofing:

The hacker/program can masquerade as another data and eventually gets access to the system as a legitimate user. All these attacks can be done using the weakness in the AMI components or the communication protocol user. E.g. Zigbee protocol do not have any
security checks once you are a part of a network. So, if the attacker gains access to one machine he/she can easily affect all the other components in the network easily.

3.6 Denial of Service:
It is an attempt to make AMI system resources unavailable to its intended users. In this type of attack an attacker gains access to one of the smart meters on the customer side. It can affect other systems in the network (e.g Smart Meter1 upto smart Meter50). After gaining access to the system, it will demand high energy consumption. Thus, it will exhaust resources by false demands of energy. In another case, the user can deploy a malicious program within the network. The program will constantly demand false energy requests and thus exhausting the resources. In this situation, the legitimate user may miss the requested resources. This can be done in several ways through resource exhaustion and integrity violation. In integrity violation hacker can modify the AMI data and thus prevents intended users from using the AMI system resources. Denial of service compromises the availability of requested resources.

3.7 Denial of action:
User or utilities can deny action/service after the request. This will affect the accountability or non repudiation of the data. Non repudiation can affect customer’s image or business of utilities. This can be performed in many ways:
Stolen/Altered: The AMI data could be stolen or altered and that could lead to denial of action that took place or claim of an action that did not take place.
Repudiation: People, including public authorities, may refuse to acknowledge an action that took place. Customer can deny after requesting the energy resources to save money. Thus, this is one of the important aspect while configuring the AMI or the AMI network.

3.8 Insider Attack:
The insider attacker would take advantage of access to systems at the opposite end of the AMI system from the customer endpoint. The systems that the attacker has access to may include the AMI head-end. AMI head-end provides the pricing information for the resources from Independent service providers or other energy management systems. They can change the pricing information in transmission. Thus, customer will have modified pricing information. This can lead to legal issue with customers or utilities responsible for. This can affect confidentiality, Integrity, availability and accountability of data.

3.9 Unauthorized Access from Customer Side:
One of the risks with AMI is that it can provide access to the electric grid from customer side. The attacker can get access to the network by above defined attacks/techniques. The attacker can access one of the endpoints in AMI by hacking the wireless communication.

3.10 Customer Cheating:
AMI enables customers to interact with Smart meters to provide energy usage to utilities. There is a big concern for customer cheating to those meters reduce the bills. Customer threat is one of the big concerns while developing the AMI system as customer can
modify the data to reduce the usage bills. Customer can reset the meter or modify/program the meter not to record the usage. It can also change the price signal rates and later deny of receiving the original price rates. Thus, integrity and non-repudiation is big concern with customer cheating. Thus, while creating AMI meters, there should be some way of verifying non-repudiation. Further, there should be some limitations/restrictions to what customer can access.

As explained above, AMI is vulnerable to many security threats, which can cause disasters (E.g. power outage in mission critical infrastructure). Therefore, the AMI manufacturers should follow certain standards and best practices to mitigate those security risks. The following chapter will highlight some of the best practices that can be used to protect AMI against the security risks.

3.11 Malicious Update/Patches:
AMI manufactures have to update the underlying metering firmware/software to update them with latest thread. The biggest issue while applying patches would be to check the integrity of the patch/updates. When the AMI manufactures sends an update code, the meter should perform some integrity checks before downloading and applying the changes. The attacker might spoof the submitted code by the manufacture and add some malicious code. If there is no integrity check before downloading the code, the malicious code by user can be effective. This type of attack compromises the integrity and confidentiality of the data.
3.12 Authenticating and Authorizing Maintenance Personnel to SM:

Smart meter deployments have passwords deployed in the meters. These passwords are different from the user password while accessing the smart meters. Although this passwords are shared to the users and the other related entities for the deployment process. By sniffing or social engineering, the attacker can get access to the password. After having the credentials, the attacker can infect the whole deployment process and other communicating entities in AMI.

By-pass authentication to/from AMI Head Ends

It’s crucial to validate the communication before it’s sent to the AMI head-end. Attacker cans by-pass the authentication using some the weaknesses in the code (e.g. SQL Injection). Once the attacker establishes a communication, it can change the price signals or can reset the meter data. Further, attacker can also perform different attacks explained previously to harm the AMI system.
Chapter 4

AMI SECURITY BEST PRACTICES IN GENERAL

Utilities are spending considerable amount of resources to develop Advance Metering Infrastructure systems. AMI manufactures are visioning for reduced energy usage by properly managing energy needs by customers.

AMI has several benefits including filed operations, load forecasting, meter management and several areas such as: customer care, power outage management, reducing dependence on non-renewable resources lowering exposure to spot market energy pricing and moderating greenhouse gas emissions. Further, it also covers consumer benefits such as: allowing utilities the ability to provide consumers with real-time energy monitoring and Demand Response programs, dynamic energy pricing and new energy management services. Thus, consumer saves money on their bills.

As, technology progresses, it comes with potential risks and issues especially in terms of security. As the first phase discussed potential security risks for AMI, this phase, will discuss best practices to mitigate those security risks, which will benefit the AMI Utilities.

4.1 Basic AMI Cryptography Considerations

Security requirements for AMI are based on confidentiality and privacy, integrity, availability, non-repudiation/accounting and authentication. The basic functionality is
based on cryptographic key and it’s management. As discussed in the above chapter, hacker’s access to one of the component of AMI system can cause serious issues to the smart grid infrastructure.

Cryptographic authentication should be enforced before accessing any devices in the network. Further, all the communication within AMI should be encrypted. Providing the integrity checks to the meter will verify that unauthorized/legitimate users do not temper the meter data. Encryption can mitigate some of the listening, eavesdropping and traffic analysis attacks. Thus, the meter data should be encrypted with efficient encryption algorithm. Whenever there is software upgrade required, verifying the integrity checks will ensure that the software is not being tempered by attackers. Performing meter auditing at customer site will help to avoid any customer cheat or hacker activity. One of the biggest concerns with AMI is customer cheat. Integrity checks can provide a way to see if the customer/hacker tempers the meter. All the pricing signals and energy demands should be encrypted. Further, the requests should have the integrity check at both ends. Logging all the user interactions with the meter would help to ensure non-repudiation. Strong firewalls, virus and malware detectors will help against any malicious program in the system. Further, the system keys should be protected. Implementing role-based control will help to separate the user activities.

4.2 Code Signing and Firmware Authentication:

Code signing [6]
Code signing is a process in which certificate based digital signature is used to validate the identity of the individual. Signed certificate can provide a way to authenticate legitimate user. After validating the identity, by checking the authenticity of the signer (trust-based relation) of the certificate, the users are allowed to use the devices/meter. For generating the certificate, it requires public-private key pair is required. The author owns the private key and only the author knows it. The public key is sent to the certificate authority (CA). After receiving the public key of the author and certificate request, the CA will generate the trust certificate for the author. Once the trust certificate is generated for the author, the developer can provide the private key to sign the code and submit it. When developer submits any changes to the code, it’s always signed as specified above. So at the customer site, customer tries to download any patches/updates, the code comes as a digitally signed. Thus, the user can verify that the update/patches are from the legitimated source.

When code is signed below steps are taken to ensure integrity: Developer creates public-private key pair. The code would be passed to the hash function, which creates a message digest. The digest is encrypted by the developer using his private key to ensure integrity. Once the digest is encrypted, it’s combined with the certificate created using public key of the developer. This code is sent to the customer site. When customer receives this patch/update code, first the code is validated by checking the certificate associated with it. Public key of the developer (from the CA) is used to validate the code. The message digest is decrypted using the public key of the developer. Further the hash function (same as the one used by the developer to create the message digest) is used to create another
message digest. This digest is validated by checking it with the original to see the integrity. If both the digests are different that means that it code has been changed during the transmission.

4.3 Against Customer Threat:
Customer threat is a biggest concern for AMI manufactures. Strong checks should be implemented to check every activity of the customer. AMI authorities should provide data transmission standard so that the customer cannot compromise those data.

The AMI industry and operators could mount an effective defense against abusive customers by using a data transmission standard for AMI data and investigating abnormal usage patterns. In addition to that, customer endpoint as access to exploit the AMI network can be prevented by implementing network control defenses such as router access lists and firewalls within the AMI network. When doing so, the utility will need to consider each of the points at which the communication changes networks to ensure that attackers can’t bypass defenses by jumping into the middle of the network. Some AMI architectures call for several transitions from one communication network to another, including wireless communication at points upstream from the customer endpoint.

4.4 The terrorist and Nation-state Threats:
They can be mitigated by all of the above because they make the target less attractive. Additional effective approaches to protecting against this threat are router access lists,
firewalls, protected communication between the AMI network and other networks, strong communication authentication, and detection and halting of rapid market fluctuations.

4.5 Information Security policies:

Information security policy specifies high level plans including establishment of Information security officer, operational security procedures such as user and data authentication, backup policies etc. There is also an implementation guide which describes how the information security plans will be implemented. Enforcement and auditing, including penalties for violation, makes sure that security policies, plans, and implementation, are handled correctly. In the smart grid, these policy documents can be created in a straightforward manner and submitted to upper management for approval.

4.6 Software Updates and Patches:

Software updates and patches are needed because the software is not secure. Attackers are always searching for vulnerabilities in the system to attack it. Thus, software should be up to date to mitigate those security attacks. That can be done by applying patches and updates to the software. If patches and updates are not done, vulnerabilities are exponentially increased. Patch management procedures and frequency of the updates must be documented. Although this can be done in the smart grid there are problems. For instance specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems in the smart grid. Their accessibility for software upgrades or patches maybe a complex activity since the equipment is typically
distributed and isolated. Additionally, the patch, test and deploy lifecycle is fundamentally different in the electrical sector. It can take a year or more to go through a qualification of a patch or upgrade. Because deployment of a security upgrade or patch is unlikely to be as rapid as in the IT industry there needs to be a process whereby the risk and impact of vulnerability can be determined in order to prioritize upgrades. Also a security infrastructure needs to be in place that can mitigate possible threats until the upgrade can be qualified and deployed so that the reliability of the system can be maintained.

Another issue is to ensure that the updates are done securely since they will likely be done online to prevent expensive physical visits to equipment. Therefore, it is critical to assure that firmware update mechanisms are not used to install malware. This can be done with a combination of strong authentication/authorization mechanisms for the person performing updates, integrity mechanism to ensure that the firmware is secure, and remote attestation mechanisms to ensure that the correct version is being updated. Finally, there should be ways to detect tampering.

4.7 Physical Security:

Having rules about who can physically access an asset (information or equipment) and how they gain entry can decrease the likelihood that an unauthorized individual is present to access information. Additionally, policy documents should discuss how a physical asset is stored and destroyed.
In the Smart grid infrastructure this best practice can be applied to the business, and some operational entities. On the other hand, in the case of smart meters for instance it is difficult to maintain physical security so one has to assume that an attacker can gain physical access to it. This means that the meter should be made tamper-resistant or tamper-evident. Ability to make a cost-effective tamper-resistant meter is not an easy problem.

4.8 Data Classification and Retention:

Data classification refers to classifying data according their security (confidentiality, integrity, or availability) level. Retention refers to how long data is kept before destroyed. The purpose of this best practice is to reduce an organization’s liability by classifying exactly what type of data is needed and how long it is needed. For example there have been cases where a breach occurred and sensitive data (credit card number) which had no business need of being kept was stolen.

In the smart grid this principle can be used in the business side of the smart grid in a straightforward manner. However in the operational and distribution side it could be a problem because there could be energy data about a customer that could reside in a meter, meter data management system, or AMI headend. Meter data especially is unattended. Clearly, there are privacy issues that apply. Another issue is what happens to meter data when a house changes hands. The NIST smart grid privacy group is currently looking at these problems. Future documents will address these problems in more detail.
4.9 Employee Awareness, Training, and Education:

How well informed employees are about security issues can help to identify or prevent a security incident. The old adage ‘security is based on the weakest link’ makes this imperative. In many respects each employee is a member of an organization’s security army. Training is needed, and expectations should be set appropriately and communicated clearly in a policy. There are different levels of training. There is awareness training and technical training depending on employee background and job classification.

In the smart grid this best practice can be applied in a straightforward manner.

4.10 Incident Response:

Incident response is important because a breach is inevitable since no system can be 100% secure. Incident response procedures should be developed so that it is used in the event of an incident. Incident response includes disaster-recovery and business-continuity plans. To response to an incident the incident must be detected. In traditional IT systems incidents can be detected with firewalls and/or intrusion detection systems that use a database of past attack signatures. Machine level intrusion typically involves using hashes of known system software.

In the smart grid these methods can be used in the business side of systems. In the operation, distribution, and customer level, the methods mentioned above cannot be applied directly. For instance a smart meter will typically not have enough memory or computational power to store the database of attack signatures. Additionally, because of
the millions of devices involved there could be too much network traffic if the devices have to access an external database. Finally, because the smart grid is a control system as well as critical infrastructure it is beneficial to employ real time intrusion detection. This is different from classical IT systems where intrusion is detected and the response is done after the fact. In the smart grid one wants to be able to respond to incidents without shutting systems down. Further research is needed in these areas and will be discussed in the future documents.

4.11 Password Requirements and Guidelines:
Employees dread having another password to remember. The more complicated requirements are made to ensure password security, the more employees decide to write them down and consequently expose them to others. It is good to establish a strong password policy but stay within reason for employees. Sometimes, additional training on teaching employees how to choose good passwords and recognition of social engineering techniques attackers use to obtain passwords will help.

4.12 Threat Modeling:
Threat model is a set of possible security attacks on the system or software. In threat modeling first the security requirements are identified. After identifying the requirements, the software is created to meet the defined requirements. At the same time security team will come up with possible attack patterns to validate confidentiality, accountability, non-repudiation and integrity. This will help to understand potential risks to the software. The
same approach can be used to protect AMI against security risks. AMI manufactures should come up with a threat model to identify hidden attacks on the Smart meters, communication protocols etc. This will help the manufacturers to identify risks in early stages before deployment at customer site.

Next chapter will describe the best practices according to different areas of security and different components of AMI.
As discussed in the previous chapter, security threats to AMI can cause high risk. AMI should be designed using some standards that include the basic to extended security coverage against threats.

5.1 Social Engineering:
Social Engineering is a big concern in security now days. The attacker can reveal the secret information by social engineering. Thus, all the entities involved in AMI should be trained against different methods of social engineering. Providing strong passwords, pass phrase will help against guessing the password. Further, security questions should be set to the values that no one can guess (E.g. First School – xyz). Provide the information that nobody can guess. Further, physical security is one of the concerns. Insider attacker can deploy webcams, key loggers to your machine and can easily get access to the information you are typing. Proper care should be taken to mitigate these risks e.g. involving biometrics authentication to uniquely identify people.

5.2 Admin Threats:
Administrative threats can be caused by poor management by administrators. To mitigate this type of risks are as follows: Roll-based access control can be used to validate that authenticated administrators gets what they are allowed to. E.g., if the admin1 is allowed
send only price signals; make sure that the admin1 should have access to no other information then he is allowed to. Malicious administrator can affect the system badly as they have access to wide range of data. Thus, all the activities by administrator should be logged so that later they cannot deny later about their activities. Further, admin session protection is one of the concerns. Attackers can user some of the listening attacks to the admin activities and easily get access to the sessions. Thus, strong session protection should be established within AMI. Whenever the credentials are passed over the network, there should be strong encryption performed before they are transferred. Proper use of phishing filters, firewalls will provide additional protection. Some additional best practices include changing the security policy database and enforce security checks to confirm the admin rights. Separation of concerns would help to differentiate between levels of access to each admins. Whenever admin submit any changes or information to the meters, it should be digitally signed to validate the identity. Further, it ensures that the data is not compromised during the transmission. Above suggestions would help to ensure confidentiality, integrity and accountability of the data.

5.3 Audit Threats:
Logs provide useful information about the events/communications/logons in the system. It helps to achieve non-repudiation of data where one cannot deny after performing some activity. So, the logs should be protected from any modification from unauthorized users. There should be role-based separation of concern on who can view/modify the policies for logs. As described above, strong authentication should be enforced before
accessing/modifying the logs. There should be active secondary back-ups to ensure the data protection against the log data (modifying purposely/accidently). The audit logs should be managed well so that no unauthorized user can have access to the critical data or be eligible to modify the data. Further, by providing “audit log maintenance” frequently allow better maintained audit logs. Backup audit logs are necessary to maintain the data properly and it will eliminate any threats against running out of resource space. As, the attacker might generate valid log data many times (by creating a program that request certain data many times and once reaches the certain limit, can perform malicious activities). The policies for auditing should be modified/studied frequently to make sure of any hidden by-pass rules. The policy database should be update frequently based on different threat profiles to avoid any back-doors. Whenever there are new threats published, the log rules should be updated to ensure against those threats. Threat modeling training programs would help the audit admins to understand various threats and their patterns of attack. They can modify the active audit rules to avoid any attacks.

5.4 Download Threats:
Download threats are typical caused when trying to download firmware/updates to the AMI. Appropriate security checks should be deployed at the customer side. Whenever there is a firmware/update request comes at the customer site, the authenticity of the source should be validate by checking matching the message digest of the digitally signed code. Strong code signing standard should be deployed to ensure the identity. Further,
any code should first undergo the virus/worm defender programs. Virus/worm/Trojan scanning will ensure that the data sent does not have any bad code that can harm the system. This should be done automatically once the request of change appears. This process will help to insure the confidentiality, integrity of the data. All the download activities should be logged in the system for later verification. Providing intermittent integrity checks will ensures the data modification.

5.5 Eavesdropping Threats:
Eavesdropping can or cannot be harmful. It depends on the eavesdropper’s profile: curious eavesdroppers or publicity seekers are not that harmful. Active/terrorist eavesdropper can harm Advance Metering Infrastructure. AMI components use wide variety of communication protocols to communicate within AMI components. Thus, certain secure standards should be followed during communication to ensure the integrity and confidentiality of the transmitted data. The sessions should established using strong authentication checks via secure channels. Further, phishing is one of the popular ways of eavesdropping. Thus, during a session or while downloading a firmware upgrade, phishing filters should be on to validate the identity of the source/destination. Role-based access control should be implemented to ensure the control over the transmitted data and authenticity of the sender/receiver. Using public-private key encryption will provide a way to identify the communicating parties. Restrict user access to cryptographic IT assets using roll-based access to the policies. Provide complete separation between data and keys and between plain text and encrypted data. Further, users (customer/admin etc.) play
an important role in eavesdropping. E.g. customer leave the established session unattended. The eavesdroppers can take an advantage of the established session and can harm the AMI communication. In other scenario a user leaves the AMI session token and leaves without clearing the session. So, the sessions should be cleared every time after the communication has ended. Educating the user profile would help to protect against some of the above mentioned threats. Further, the system should be able to detect any keystroke stored in the system against misuse.

5.6 Identification & Authentication Threats:

I&A threats are those threats involve the user identification and the process to authenticate the users. Brute-force is one of the technologies applied to guess the password by applying dictionary words, random combinations and permutations. Therefore, the strong password rules should be deployed when creating a password (e.g. combination of letters and numbers including special characters). Further, the credentials should be encrypted before transmitting over the AMI communication network. If the passwords are encrypted strongly, sniffers would fail to capture the password. Social-networking can be mitigated by educating the customers and all the responsible entities.

5.7 Insider Threats:

Insider threats are those threats that directly involve authorized users. We cannot neglect the fact that the users can also cause harm to the AMI. Once the user is authenticated, he/she can infect one of the systems in the communication network and thus infecting the
AMI network. E.g. creating a backdoor in the system and running virus program in the system will affect all the connected components. To mitigate these types of risks abnormal activities should be detected and actions should be taken right away. E.g. virus detectors or keystroke detectors. Publicizing the improved detection capability also reduces risk by deterring insider activity. Further, Background checks and frequent audits, strong authentication procedure, implementation of intrusion detection systems and integrity checks can help to ensure the system against any attacks. All the communication from the customer to AMI head-end and head-end to the customer endpoint should be considered as a controlled traffic. Strong authentication and sniffer detectors would help to prevent any sniffing or man-in-the-middle attacks. Head-end systems are very crucial part of the AMI as it contains the price information and other billing information. So, the AMI manufactures should follow the secure software development practices to better serve against the security attacks. There should be strong back ground check performed for those who directly deal with AMI core. As the insider attacks are hard to detect. Further, strong audit log rules will help to ensure integrity and non-repudiation of the data. All the user actions should be logged and the logs should have a backup data. Roll-base access control and separation of data would help to mitigate the intensity of the attack. Intrusion detection systems at the host site would help to validate any malicious activity within the AMI by the insider.
5.8 Malicious Code:

Malicious code can cause serious damage to AMI infrastructure. Thus, the AMI manufactures should follow a consistent secure software development life cycle to build the AMI. Secure coding practices will help to mitigate security risks. E.g. SQL Injection: one of the biggest mistakes by the developer while writing database queries. E.g. for validating the user credential the code checks for username and password. If the coder missed the magic quotes checks, then the user can provide “user&-” and space. That will be considered in database as bypassing the next field (which is password) and thus the attacker can have access to any user’s profile without providing the password. Further, strong string manipulation and boundary checks should be implemented. At the customer side, there should be strong input validation present. Further, to identify the authenticity of the code, it should be signed using digital signatures. At customer site, before downloading the code, the digest should be match to ensure the integrity of the code. Virus scans, checking the certificate should be performed before executing any executable file to avoid any malicious change to OS and important data file. All the modification should be logged under audit logs. The logs should be checked frequently to see for any malicious or unusual activity. Developer should be trained against threats to the weak coding practices. They should be educated for strong and secure coding practices.
5.9 Operational Denial of Service (DOS) attack:
It affects the availability of the system and can cause serious issues to critical infrastructures. User sessions while dealing with Smart meters for any energy request should be secured to avoid any sniffing or eavesdropping of the data. All the communications should be initiated once the user authentication is completed. All the communication from customer – Smart Meters – Customer gateway to AMI head-end should be encrypted using strong encryption algorithm. All the messages sent over the network should be digitally signed using public-private key to ensure confidentiality of the message. Once the user is authenticated using the above best practices, audit the user activities. Deploy some audit checks in the Smart Meter to detect any suspicious requests. Use above methods to ensure that the user is not exhausting the resources by making many dummy requests. Further, the Smart Meters should implement a counter to keep track of user request. The counter should have predefined threshold value so that the user cannot exceed the requests beyond the predefined threshold value.
Chapter 6

CONCLUSION

As described in the previous chapters, AMI security risks vary from low to high. Some risks to AMI can affect the Smart Grid potentially. Discussed security issues are based on confidentiality, Integrity, Authenticity and Non-repudiation. These threats are likely to change based on changes to AMI. As, AMI requirements or design is not shared in public due to security reasons, there can be areas that may have missed in the report. There are some areas of research regarding communication protocols used and underlying structure of the AMI. The security threats greatly depend on the communication protocols as the current protocols have security threats attached with them.

Best practices mentioned in this report are general best practices that can be applied to AMI. There are several areas of research in AMI. E.g. which protocol should best fit for secure AMI etc. Further, meters differ from one manufacturer to other. Thus, there is no single threat model that can server for all the meters. In addition to that, there is no clear definition on how to defend the meters against insiders, power theft etc. Some of the other research topic includes patches and update (how to deploy the update), key management – whom to trust, difficulty in retrieving keys, certificate processing complexity, physical security, Education and training, social engineering etc.
AMI is a wide topic and there can be many security issues related with it. The best way to find the security issues would be to dig into the actual meter and the communication. This will help to understand loopholes in the system and communications. Other suggestion could be to have a red-team attacking to the test environment. This will uncover hidden potential security risks in the AMI.
REFERENCES


Available: http://pc.wednus.com/Home/kb-1


Available: http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx

[5] F. M. Cleveland, Senior Member IEEE, IEEE T&D Conference, April 2008 -  
“Cyber Security Issues for Advanced Metering Infrastructure (AMI)” [Online]  