Energy Research and Development Division
FINAL PROJECT REPORT

BEST PRACTICES FOR HANDLING SMART GRID CYBER SECURITY

Prepared for: California Energy Commission
Prepared by: California State University Sacramento

MAY 2014
CEC-500-2014-049
DISCLAIMER

This report was prepared as the result of work sponsored by the California Energy Commission. It does not necessarily represent the views of the Energy Commission, its employees or the State of California. The Energy Commission, the State of California, its employees, contractors and subcontractors make no warranty, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Energy Commission nor has the California Energy Commission passed upon the accuracy or adequacy of the information in this report.
PREFACE

The California Energy Commission Energy Research and Development Division supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The Energy Research and Development Division conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The Energy Research and Development Division strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

Energy Research and Development Division funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

*Best Practices for Handling Smart Grid Cyber Security* is the final report for the Smart Grid Information Assurance and Security Technology Assessment project (contract number 500-08-027) conducted by University of California Sacramento. The information from this project contributes to Energy Research and Development Division’s Energy Systems Integration Program.

For more information about the Energy Research and Development Division, please visit the Energy Commission’s website at [www.energy.ca.gov/research/](http://www.energy.ca.gov/research/) or contact the Energy Commission at 916-327-1551.
ABSTRACT

This report discusses best practices for Smart Grid information assurance and security issues. The best practices discussed were mitigation and countermeasures used in information systems security to address threats, vulnerabilities and risks that were developed in a previous report.

The goal of the project was to:

1) Identify the potential issues affecting the confidentiality, integrity, and availability of information flow in the Smart Grid system and group the issues with respect to confidentiality, integrity and availability.

2) Investigate which information security best practice(s) apply to the Smart Grid and to what extent they could be applied. These best practices were intended to mitigate actions that violated confidentiality, integrity, and information flow availability.

3) Explore possible cyber security research and development issues that should be addressed in the Smart Grid, such as wireless sensors, wireless communication systems, monitoring and incident response systems.

4) Identify and recommend which potential research and development efforts should and should not be confidential.

5) Identify technical and non-technical solutions to ensure the privacy of end user information.

Researchers used information from various Smart Grid working groups that were dealing with cyber security issues, including Utility Security, Open Smart Grid, National Institute of Standards and Technology and Intelligrid. Information was also obtained from web sources, journals and magazines.

The results showed that in some cases information security best practices used in conventional information technology systems could be used to address Smart Grid vulnerabilities. They could be used directly in some cases (e.g., security policy creation), but there were other situations where they could not. There were also situations (e.g., intrusion detection) where further research will be needed to address security issues because of the unique characteristics of the Smart Grid as a critical infrastructure. Researchers plan to report on these research issues in another document.

Keywords: Public Interest Energy Research, PIER, smart grid, electric grid, cyber security, critical infrastructure, information assurance, best practices, countermeasure

Please use the following citation for this report:

# TABLE OF CONTENTS

PREFACE ............................................................................................................................... i

ABSTRACT ............................................................................................................................... ii

TABLE OF CONTENTS .............................................................................................................. iii

LIST OF FIGURES .................................................................................................................... vii

LIST OF TABLES ..................................................................................................................... viii

EXECUTIVE SUMMARY ............................................................................................................. 1

Introduction ........................................................................................................................... 1

Project Purpose ....................................................................................................................... 1

Project Results ......................................................................................................................... 1

Project Benefits ....................................................................................................................... 2

CHAPTER 1: IT Best Practices for Smart Grid Cyber Security ................................................... 4

1.1 Introduction ....................................................................................................................... 4

1.2 General Best Practices for Securing IT Systems ................................................................. 5

1.2.1 The Information Security Policy .................................................................................. 5

1.2.2 Software Updates and Patches ................................................................................... 5

1.2.3 Physical Security ......................................................................................................... 6

1.2.4 Data Classification and Retention ............................................................................... 6

1.2.5 Employee Awareness, Training, and Education ......................................................... 6

1.2.6 Incident Response ....................................................................................................... 7

1.2.7 Supply Chain Management ......................................................................................... 7

1.2.8 Password Requirements and Guidelines ................................................................. 7

1.3 System Life-Cycle Management ....................................................................................... 8

1.4 Technical Best Practices for Handling Violations to Confidentiality, Integrity, Availability, and Accountability ................................................................. 22

1.5 Secure System Design Principles ................................................................................... 30

1.6 Conclusion ....................................................................................................................... 32

CHAPTER 2: Demand Response Practices ............................................................................... 33
3.4 Gateway ............................................................................................................................... 61
  3.4.1 Best Practices for Gateway .......................................................................................... 61
3.5 Home Area Network ............................................................................................................. 62
  3.5.1 General Best Practices for ZigBee ................................................................................ 63
3.6 Comprehensive Best Practices for Securities with HAN/Gateway/ WNAN ....................... 65

CHAPTER 4: Advanced Metering Infrastructure (AMI) .............................................................. 67
  4.1 Introduction .......................................................................................................................... 67
  4.2 AMI Security Best Practices ........................................................................................... 68
  4.3 Basic AMI Security Considerations: .................................................................................. 69
    4.3.1 Code Signing and Firmware Authentication ............................................................... 70
  4.4 Best Practices for the Security Issues .............................................................................. 71
    4.4.1 For Customer Threat .................................................................................................... 71
    4.4.2 The Terrorist and Nation-State Threats ...................................................................... 71
  4.5 Best Practices for Different Areas of Security ................................................................. 72
    4.5.1 Admin Threats ............................................................................................................ 79
    4.5.2 Audit Threats ............................................................................................................. 81
    4.5.3 Download Threats ....................................................................................................... 83
    4.5.4 Eavesdropping Threats ............................................................................................. 83
    4.5.5 Identification & Authentication Threats ....................................................................... 85
    4.5.6 Insider Threats ............................................................................................................ 86
    4.5.7 Key Management Threats .......................................................................................... 87
    4.5.8 Malicious code ........................................................................................................... 88
    4.5.9 Operational Denial of Service (DOS) Attack ............................................................... 91
    4.5.10 Operational integrity threats ..................................................................................... 94
    4.5.11 Operational Non-Repudiation Threats ..................................................................... 95
    4.5.12 Social Engineering Threats: ..................................................................................... 96
    4.5.13 Flawed Implementation Threats: ............................................................................... 98

CHAPTER 5: Countermeasures for SCADA Vulnerabilities ....................................................... 99
CHAPTER 5: Countermeasures for Master Terminal Unit and Remote Terminal Unit Security Issues:

5.1 Countermeasures for Master Terminal Unit and Remote Terminal Unit Security Issues: 

5.1.1 Counter Measures for Policy and Procedure Vulnerabilities: ............................................ 100
5.1.2 Regular Vulnerability Assessments ........................................................................... 102
5.1.3 Expert Information Security Architecture Design ....................................................... 102
5.1.4 Implement the Security Features Provided by Device and System Vendors .......... 102
5.1.5 Establish Strong Controls over Any Medium That Is Used as a Backdoor into the SCADA Network ................................................................................................................ 102
5.1.6 Implement Internal and External Intrusion Detection Systems and Establish 24-Hour-a-Day Incident Monitoring ................................................................................. 102
5.1.7 Conduct Physical Security Surveys and Assess All Remote Sites Connected to the SCADA Network ................................................................................................................ 103
5.1.8 Firewalls and Intrusion Detection System ................................................................. 103
5.1.9 Electronic Perimeter .................................................................................................... 104
5.1.10 Domain-Specific IDS ............................................................................................. 105
5.1.11 Creating Demilitarized Zones (DMZs) .................................................................. 105
5.1.13 Low Latency and High Integrity Security Solution Using Bump In the Wire Technology for Legacy SCADA Systems .................................................................................... 106

5.2 Countermeasures for Enhancing DNP3 Security: ......................................................... 107

5.2.1 Countermeasures ........................................................................................................ 108
5.2.2 Solutions That Wrap the DNP3 Protocols without Making Changes to the Protocols ............................................................................................................................. 108
5.2.3 Enhancements to DNP3 Applications ........................................................................ 109
5.2.4 Distributed Network Protocol Version 3 Security (DNPSec) ................................... 111
5.2.5 Comparisons of DNP3 Countermeasures ................................................................ 118
5.2.6 Conclusion ................................................................................................................ 120

5.3 Countermeasures for Enhancing Modbus Security ......................................................... 120

5.3.1 Secure Modbus Protocol ............................................................................................ 121

CHAPTER 6: Plug-in Hybrid Electric Vehicles ....................................................................... 126

6.1 Introduction .................................................................................................................... 126
6.2 PHEV Charging and its Impact: ............................................................................. 127
6.2.1 Battery Charging ............................................................................................... 127
6.2.2 Direct Charging and Its Impact on the Electricity Grid ..................................... 127
6.3 Security Issues and Counter Measures: .................................................................. 130
6.3.1 Privacy ............................................................................................................. 130
6.3.2 Secure Payment ............................................................................................... 130
6.3.3 Smart Metering ................................................................................................ 131
6.3.4 Critical Infrastructure and Physical Security ..................................................... 132
6.4 Tamper-Resistant .................................................................................................. 133
6.5 Communication ..................................................................................................... 133
6.6 Security Issues with Networking: ......................................................................... 133
6.6.1 Cross Platform/Networking Systems .................................................................. 134
6.6.2 Internet 3G Cross Network ............................................................................. 135

CHAPTER 7: DER ............................................................................................................ 136
7.1 Physical Security: .................................................................................................. 138
7.2 Cyber Security ...................................................................................................... 139

GLOSSARY ...................................................................................................................... 142

REFERENCES ................................................................................................................ 147

LIST OF FIGURES

Figure 1.1: Conceptual View of SDLC .......................................................................... 8
Figure 1.2: Public Key Encryption ............................................................................... 24
Figure 1.3: Message Authentication Code .................................................................... 25
Figure 1.4: Signature Generation and Verification ....................................................... 26
Figure 2.1: Subsystems & Networks in a Sensor Network Based DR Architecture ........ 35
Figure 2.2: Simplified RSA-Based and ECC-Based SSL Handshake with Mutual Authentication.
Pay Load Message Size in Byte [RSA, ECC] ............................................................... 38
Figure 2.3: Zigbee Layer Model .................................................................................. 41
Figure 2.4: ZigBee-Based HAN Enabling Demand Response from Utilities Network .... 42
Figure 2.5: TLS Handshake with Client Certificate and MITM Attack ......................... 48
Figure 2.6: Asymmetric Cryptography ........................................................................ 49
Figure 2.7: Authentication Using X.509 Certificate ..................................................... 50
Figure 2.8: The Signing and Verification Process of Digital Signature ....................... 51
Figure 2.9: Requesting and Obtaining Process for X.509 Certificate ......................... 53
Figure 2.10: Path of Attack in PCT System ................................................................. 54
Figure 2.11: Defend Mechanisms for PCT Systems .................................................. 55
Figure 2.12: Hierarchy of the Key Distribution ....................................................... 56
Figure 3.1: Customer Domain which includes WNAN, gateway and HAN .................. 58
Figure 4.1: AMI Components. Source: Open Smart Grid; Shared Documents; .......... 68
Figure 5.1: Basic Functions of Security Policy ......................................................... 101
Figure 5.2: Firewall and Intrusion Detection System Implementation between Enterprise and SCADA Control System ........................................................................ 104
Figure 5.3: Electronic Perimeter Implementation in SCADA System ......................... 105
Figure 5.4: Demilitarized Zones Architecture ......................................................... 106
Figure 5.5: Model for Bump in the Wire Approach .................................................. 107
Figure 5.6: Protocol Stack (Gray-Background Protocols Are Secured Alternatives) ....... 109
Figure 5.7: Authentication Using Authentication Octets .......................................... 110
Figure 5.8 DNP3 Protocol Structure ....................................................................... 112
Figure 5.9: Message Sequence in Challenge Response ............................................ 115
Figure 5.10: Message Sequence in Aggressive Mode .............................................. 115
Figure 5.11: DNP3 Request/Response Link Communications .................................... 117
Figure 5.12: Message Sequence in Key Management .............................................. 118
Figure 5.13: Secure Modbus Application Data Unit .................................................. 122
Figure 5.14: Modbus Secure Gateway ..................................................................... 122
Figure 5.15: High Level Secure Survivable Architecture ......................................... 124
Figure 6.1: Power Output Determines the Charging Times ........................................ 128
Figure 6.2: Power Variance Based on Charging Method and Time ............................ 129
Figure 7.1: Architecture for Proposed Integrated Smart Grid Systems ..................... 136

LIST OF TABLES

Table 1.1: Initiate Security Planning ......................................................................... 10
Table 1.2: Assess the Impact of Privacy .................................................................... 10
Table 1.3: Ensure Use of Secure Information System Development Processes ........... 11
Table 1.4: Assess the Risks to the System ................................................................. 12
Table 1.5: Select and Document Security Controls.................................................... 13
Table 1.6: Design a Security Architecture ................................................................. 14
Table 1.7: Develop a Security Documentation ........................................................... 15
Table 1.8: Conduct Testing ....................................................................................... 15
Table 1.9: Create a Detailed Plan for Authorizing Officials ....................................... 16
Table 1.10: Integrate Security into the Established System ........................................ 17
Table 1.11: Assess System Security .......................................................................... 17
Table 1.12: Review Operational Readiness ............................................................... 18
Table 1.13: Perform Configuration Management and Control .................................. 19
Table 1.14: Conduct Continuous Monitoring ............................................................. 20
Table 1.15: Build and Execute a Disposal .................................................................. 21
Table 1.16: Ensure Information Preservation ............................................................. 21
Table 1.17: Dispose of Hardware and Software ................................................................. 22
Table 3.1: Comprehensive Best Practices for Securities with HAN/Gateway/ WNAN .......... 66
Table 4.1: Best Practices for Different Areas of Security .................................................. 76
Table 4.2: Best Practices for Different Areas of Security ............................................... 78
Table 4.3: Admin Threats: Best Practices ........................................................................ 81
Table 4.4: Audit Threats: Best Practices ......................................................................... 82
Table 4.5: Downloading Threats: Best Practices ............................................................. 83
Table 4.6: Eavesdropping Threats: Best Practices ......................................................... 85
Table 4.7: Identification and Authentication Threats: Best Practices .............................. 86
Table 4.8: Insider Threats: Best Practices ...................................................................... 87
Table 4.9: Key Management Threats: Best Practices ...................................................... 88
Table 4.10: Malicious Code Threats: Best Practices ....................................................... 91
Table 4.11: Operational Denial of Service Attacks: Best Practices ................................. 94
Table 4.12: Operational Integrity Threats: Best Practices .............................................. 95
Table 4.13: Operational Non-Repudiation Threats: Best Practices ................................. 96
Table 4.14: Social Engineering Threats: Best Practices ................................................. 98
Table 4.15: Flawed Implementation Threats: Best Practices .......................................... 98
Table 5.1: Comparison of Security Approaches .............................................................. 111
Table 5.2: Comparisons of DNP3 Countermeasures ...................................................... 119
Table 6.1: Categories of Attacks in CPS ......................................................................... 134
Table 6.2: Attacks and Counter Measures on Internet 3G Cross Networks .................... 135
Table 7.1: Threats and Their Impact .............................................................................. 141
EXECUTIVE SUMMARY

Introduction
The intent of information security best practices is to limit successful exploitation of vulnerabilities in a system, because no system can be completely secure. Most best practices for securing information technology (IT) systems can be applied to the Smart Grid, but there are potential problems that are unique to the Smart Grid.

Project Purpose
The main goal of the project was to determine information assurance, security, and privacy issues associated with Smart Grid infrastructure and recommend research and development (R&D) priorities in those areas. Another goal was to identify information security best practices that could be applied to the Smart Grid system.

Project Results
This report is the first in a series of research documents covering cyber security issues for the Smart Grid, including:

1. Potential threats, vulnerabilities and risks.
2. Best practices to mitigate those risks.
3. Research issues to be addressed in Smart Grid cyber security.
4. Privacy issues in Smart Grid infrastructure.

This research specifically focused on best practices for dealing with cyber security issues of the Smart Grid in general and for the following Smart Grid components: advanced metering infrastructure; demand response systems; home area networks (HANs); neighborhood area networks that connect the home to utility systems; supervisory control and data acquisition (SCADA) systems that are used for controlling generation, transmission and distribution systems; and plug-in electric vehicles.

To achieve these objectives the researchers:

5. Participated and in some cases coordinated conference calls and face-to-face meetings with Smart Grid experts.
6. Attended workshops on demand response research, Smart Grid cyber security standards and Smart Grid interoperability.
7. Performed a literature search on the web.
8. Interviewed utility experts on electricity generation, transmission, and distribution processes.

The results showed that in some cases information security best practices used in conventional IT systems could be used to address Smart Grid vulnerabilities. In some cases such as security policy creation they could be used directly, but there were other situations where they could not. There were also situations (e.g., intrusion detection) where further research will be needed.
to address security issues that were unique characteristics of the Smart Grid. The researchers plan to report on these research issues in another document.

**Project Benefits**
This project helped to:

9. Increase customer trust in the Smart Grid.
10. Increase regulators’ understanding of the security issues in the Smart Grid that need to be addressed by manufacturers and utilities.
11. Increase understanding of the privacy issues in the Smart Grid and how they could be addressed.
12. Identify security and privacy issues in the Smart Grid infrastructure and propose solutions and research areas to be examined. This could help enable acceptance of wide deployment of the Smart Grid, which could help to increase energy efficiency and lower energy costs.
CHAPTER 1: IT Best Practices for Smart Grid Cyber Security

1.1 Introduction

This document is the second of a series of documents of covering Smart Grid Cyber Security Issues researched by Smart Grid Research Group which is part of the Center for Information Assurance and Security (CIAS) at California State University Sacramento (CSUS). CIAS collaborates with the Universities’ Smart Grid Center with respect to Cyber Security and Interoperability issues of the Smart Grid. This current report is about information security best practices that can be used to deal with smart grid threats, vulnerabilities and risks. That is, it covers mitigation and countermeasures to address those vulnerabilities. Unless otherwise stated the terms mitigation, countermeasure and best practices are used interchangeably in this document. The vulnerabilities were covered in the first report, Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks.¹

As mentioned above, this report is the second of a series of research tasks specified in a statement of work for the California Energy commission as follows:

1) Identify the potential issues affecting the confidentiality, integrity, and availability of information flow in the Smart Grid system. For instance, hacker/terrorist use of malicious software to perform denial of service attacks on critical infrastructure such as the Smart Grid will be examined. Group the issues with respect to confidentiality, integrity, and availability.

2) Investigate which information security best practice(s) apply to smart grid and to what extent can they be applied. 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 arena. These best practices are intended to mitigate actions that violate confidentiality, integrity, and availability of the information flow in the smart grid.

3) Explore possible cyber security R&D issues that should be addressed in Smart Grid. Some of these could involve wireless sensors, wireless communication systems, monitoring, and incident response systems.

4) Identify and recommend which potential R&D efforts should and should not be confidential.

5) Identify technical and non-technical solutions to ensure the privacy of end user information. Because Smart Grid systems will contain end user information, privacy is critical.

This report is about the second task listed above. Subsequent reports will discuss other tasks.

Best practices for securing information systems can be found in a number of standards including NIST (NIST pub 800-14, ISO 27002, RFC 2196, etc.) In the area of Smart Grid some best practices can be found in NERC CIP 002-009. A summary of some of these standards can be found in Wikipedia.²

The intent of the best practices is to limit successful exploitation of vulnerabilities in a system because no system can be 100 percent secure. Although most of the best practices for securing IT systems can be applied to the Smart Grid, there are potential problems, most of which are discussed in the NIST Bottom up Cyber Security document.³ In the following summary of Information Security Best Practices (not necessarily in priority order) some of the problems are mentioned as needed. For each best practice mentioned comments are made as to what extent the security best practice can be applied to the smart grid. Some of these problems might require further research. This is stated where necessary. Subsequent reports will delve into more details on possible cyber security R&D (research and development) issues that should be addressed in Smart Grid.

1.2 General Best Practices for Securing IT Systems

1.2.1 The Information Security Policy

Information security policy details 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 violations, ensure that security policies, plans, and implementations are handled correctly. In the smart grid, these documents can be created in a straight forward manner and submitted to upper management for approval.

1.2.2 Software Updates and Patches

Software updates and patches are needed because software is usually not 100 percent secure. Attackers are finding new ways to exploit systems. Software to defend against new exploits must be used to update systems. Vendor patches from vendors and antivirus must be used to close the security holes. 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


³ http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCCTGBottomUp
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. 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.

1.2.3 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 physical asset is stored and destroyed.

In the Smart grid infrastructure this best practice can be applied to the business, and some operational entities. 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 can be made tamper-resistant or tamper-evident. Ability to make a cost-effective tamper-resistant meter is not an easy problem.

1.2.4 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 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. 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, 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.

1.2.5 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.

1.2.6 Incident Response

Incident response is important because a breach is inevitable since no system can be 100 percent 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 will 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.

1.2.7 Supply Chain Management

Security of a system is only as strong as the weakest link, and when an organization works with third-party providers their information security downfall can become their issue. Therefore, the organization should make sure to document for instance, which vendors receive confidential information and how this information is treated when in the custody of the vendor. The lack of strict vendor guidelines could increase the risk of releasing customers’ private information.

In the smart grid this principle can be used in a straightforward manner in both business systems and customer domain to handle confidentiality. Another area where this principle is applicable is where integrity is managed in the supply chain. For instance, if a utility purchases a smart meter from a vendor, how does the utility know that the firmware is free of malware (perhaps inserted by a disgruntled employee), or that it cannot be exploited by an attacker’s malware? This problem can be handled by documented agreement, review of vendor design and manufacturing processes, thorough testing of the meter through vulnerability assessment, vendor reputation, etc.

1.2.8 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. Additionally, training employees as to why the policy is the way it is can go a long towards gaining employee acceptance.

1.3 System Life-Cycle Management

System Life-Cycle Management in systems engineering and software engineering, is the process of creating or altering systems, and the models and methodologies that people use to develop these systems. There are five basic stages in a ‘System Development Life Cycle’. This cycle refers to the entire path that needs to be followed while developing a product, ensuring maximum success of the product and a minimum chance of a failure. Such a life cycle has also been introduced in the security domain, it is known as the “Security Design Life Cycle (SDLC)”. Figure-1.1 shows a typical system development life cycle. The five stages of SDLC are described below.

![Conceptual View of SDLC](image)

Figure 1.1: Conceptual View of SDLC

---

Stage 1: Initiation:

During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. Early planning and awareness will result in cost and timesaving through proper risk management planning. Security discussions should be performed as part of the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project.

Three essential steps to be followed in this Initiation phase they are summarized in Table 1.1, Table 1.2 and Table 1.3.

1. Initiate Security Planning;

<table>
<thead>
<tr>
<th>Description</th>
<th>Security planning should begin in the initiation phase by:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Identifying key security roles for the system development;</td>
</tr>
<tr>
<td></td>
<td>• Identifying sources of security requirements, such as relevant laws, regulations, and standards;</td>
</tr>
<tr>
<td></td>
<td>• Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements; and</td>
</tr>
<tr>
<td></td>
<td>• Outlining initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching.</td>
</tr>
</tbody>
</table>

This early involvement will enable the developers to plan security requirements and associated constraints into the project. It also reminds project leaders that many decisions being made have security implications that should be weighed appropriately, as the project continues.

| Expected Outputs | • Supporting documents (slides, meeting minutes, etc.) |
|                 | • Common understanding of security expectations. |
|                 | • Initial schedule of security activities or decisions. |
**Synchronization**

A series of milestones or security meetings should be planned to discuss each of the security considerations throughout the system development.

<table>
<thead>
<tr>
<th>Table 1.1: Initiate Security Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Assess the Impact of Privacy;</td>
</tr>
</tbody>
</table>

| Description | When developing a new system, it is important to directly consider if the system will transmit, store, or create information that may be considered privacy information. This typically is identified during the security categorization process when identifying information types. Once identified as a system under development that will likely handle privacy information, the system owner should work towards identifying and implementing proper safeguards and security controls, including processes to address privacy information incident handling and reporting requirements. |
| Expected Outputs | Privacy Impact Assessment providing details on where and to what degree privacy information is collected, stored, or created within the system. |
| Synchronization | Should continue to be reviewed and updated as major decisions occur or system purpose and scope change significantly. |

<table>
<thead>
<tr>
<th>Table 1.2: Assess the Impact of Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Ensure Use of Secure Information System Development Processes;</td>
</tr>
</tbody>
</table>

| Description | Primary responsibility for application security, during early phases, lies in the hands of the development team who has the most in-depth understanding of the detailed workings of the application and ability to identify security defects in functional behavior and business process logic. They are the first level of defense and opportunity to build in security. It is important that their role not be assumed or diminished. Communicating and providing |

10
expectations is key to planning and enabling an environment that protects down to the code level. As a team, system developers and security representatives should agree on what steps can and should be taken to ensure valuable and cost-effective contributions to a secure development environment.

| Expected Outputs | • Plans for development phase security training.  
|                  | • Planned quality assurance techniques, deliverables, and milestones. 
|                  | • Development and coding standards including development environment. |

| Synchronization  | Lessons learned from completed products and security testing should be evaluated for appropriateness in adjusting development processes and standards to prevent embedding weaknesses. |

Table 0.1: Ensure Use of Secure Information System Development Processes

Stage 2: Description:

This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

- Conduct the risk assessment and use the results to supplement the baseline security controls;
- Analyze security requirements;
- Perform functional and security testing;
- Prepare initial documents for system certification and accreditation; and
- Design security architecture.

Although this section presents the information security components in a sequential top-down manner, the order of completion is not necessarily fixed. Security analysis of complex systems will need to be iterated until consistency and completeness is achieved.

There are five major steps to be followed to fulfill the requirements in this phase; the tables 1.5 to 1.8 give an overview about the steps in this stage.
1. Assess the Risks to the System:

| Description | The purpose of a risk assessment is to evaluate current knowledge of the system’s design, stated requirements, and minimal security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks. Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed. To be successful, participation is needed from people who are knowledgeable in the disciplines within the system domain. The security risk assessment should be conducted before the approval of design specifications as it may result in additional specifications or provide further justification for specifications. |
| Expected Outputs | A refined risk assessment based on a more mature system design that more accurately reflects the potential risk to the system, known weaknesses in the design, identified project constraints, and known threats to both business and IT components. In addition, previous requirements are now transitioning into system specific controls. |
| Synchronization | Since this risk assessment is completed at a more mature stage of system development, there may be a need to revisit previously completed security steps, such as BIA or Security Categorization. Development rarely goes as planned, and requirements have a way of changing. |

Table 0.2: Assess the Risks to the System

2. Select and Document Security Controls:

| Description | The selection of security controls consists of three activities: the selection of baseline security controls (including common security controls); the application of security control tailoring guidance to adjust the initial security |
control baseline; and the supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions. An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes.

<table>
<thead>
<tr>
<th>Expected Outputs</th>
<th>System Security Plan - specification of security controls that identify which, where, and how security controls will be applied.</th>
</tr>
</thead>
</table>
| Synchronization  | • Security controls and associated specifications should reflect appropriate levels of protection to the system in line with the security control selection criteria.  
• Significant decisions should consider any possible secondary risks that may result should the decision influence previously considered security controls and protections identified during the risk assessment. |

Table 0.3: Select and Document Security Controls

3. Design a Security Architecture:

| Description | At the system level, security should be architected and then engineered into the design of the system. This may be accomplished by zoning or clustering services either together or distributed for either redundancy or additional layers of protection. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users.  
This activity can provide the most value for the system in lowering the total cost of ownership by planning the systems core components in a secure way. |
|-------------|------------------------------------------------------------------------------------------------------------------------------------|
### Expected Outputs

- Schematic of security integration providing details on where, within the system, security is implemented and shared. Security architectures should be graphically depicted and detailed to the extent the reader can see where the core security controls are applied and how.
- Listing of shared services and resulting shared risk.
- Identification of common controls used by the system.

### Synchronization

- The security architecture becomes a key component of the system documentation that should be reviewed and maintained as major changes or significant milestones are reached.
- Significant results from assessments, security testing, and reviews should be examined for potential feedback on effectiveness.

### Table 0.4: Design a Security Architecture

<table>
<thead>
<tr>
<th>4. Develop a Security Documentation:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>The most prominent document is the System Security Plan. Development of these documents should consider the maturity of the security services being documented. In some cases, these documents may contain only known requirements, common controls, and templates. Filling in these documents should begin as early as possible during the project. Documenting as the system development progresses can provide cost savings and enhance decision-making capabilities through a comprehensive approach that allows early detection of gaps.</td>
</tr>
<tr>
<td><strong>Expected Outputs</strong></td>
</tr>
<tr>
<td>• Additional security documentation supporting the system security</td>
</tr>
</tbody>
</table>
These documents will need to be updated toward the end of user acceptance testing to ensure that they are accurate.

Table 0.5: Develop a Security Documentation

5. Conduct Testing;

| Description | Systems being developed or undergoing software, hardware, and/or communication modifications must be tested and evaluated prior to being implemented. The objective of the test and evaluation process is to validate that the developed system complies with the functional and security requirements. |
| Expected Outputs | Documentation of test results, including any unexpected variations discovered during testing. |
| Synchronization | All test results are returned to developers for configuration-managed updates. Unexpected results may require the customer to clarify the nature of the requirement. |

Table 0.6: Conduct Testing

Stage 3: Implementation:

Implementation/Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization’s operational environment.

Key security activities for this phase include:

- Integrate the information system into its environment;
- Plan and conduct system certification activities in synchronization with testing of security controls; and
- Complete system accreditation activities.

There are three key steps in this phase:

1. Create a Detailed Plan for Authorizing Officials;

| | The Authorizing Official (AO) is responsible for accepting the risk of operating the system; the AO can advise the development team if the |
risks associated with eventual operation of the system appear to be unacceptable. Specifications can impose excessive burden and costs if the acceptable residual risks are not known. The involvement of the AO is required for this determination of acceptable residual risks. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages. The possibility of establishing a security working group should be discussed. Such a group may consist of personnel such as users, program managers, and application sponsors; system, security, or database administrators; security officers or specialists, including the system or application analysts. To ensure proper testing and reduce the likelihood of scope creep during testing, the security accreditation boundary should be clearly delineated. This will form the basis for the test plan to be created and approved prior to implementation performance.

Table 0.7: Create a Detailed Plan for Authorizing Officials

2. Integrate Security into the Established System;

<table>
<thead>
<tr>
<th>Description</th>
<th>Expected Outputs</th>
<th>Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Work Plan: A planning document that identifies key players, project constraints, core components, scope of testing, and level of expected rigor. The certification package should be close to completion, and any initial agency-specified conformance reviews initiated.</td>
<td>ISSO provides the system owner with completed documentation required to initiate and conduct such an authorization.</td>
<td>System integration occurs at the operational site when the information system is to be deployed for operation. Integration and acceptance testing occur after information system delivery and installation. Security</td>
</tr>
</tbody>
</table>
control settings are enabled in accordance with manufacturers’ instructions, available security implementation guidance, and documented security specification.

| Expected Outputs | • Verified list of operational security controls.  
| • Completed System Documentation. |

| Synchronization | Issues encountered during installation should be evaluated for inclusion into the contingency plan based on the potential for reoccurrence. |

Table 0.8: Integrate Security into the Established System

3. Assess System Security;

| Description | Systems being developed or undergoing software, hardware, and/or communication modifications must be formally assessed prior to being granted formal accreditation. The objective of the security assessment process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk. |


| Synchronization | • Certifier provides written Certification Package results to system owner, ISSO, and system administrator.  
| • Assessment results are shared with system owner, ISSO, system administrator, and developers. |

Table 0.9: Assess System Security

Stage 4: Operations and Maintenance:

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient. Operations continue as long as the system can be effectively adapted to respond to an organization’s needs while maintaining an agreed-upon
risk level. When necessary modifications or changes are identified, the system may reenter a previous phase of the SDLC.

Key security activities for this phase include:

- Conduct an operational readiness review;
- Manage the configuration of the system;
- Institute processes and procedures for assured operations and continuous monitoring of the information system’s security controls; and
- Perform reauthorization as required.

Here again, there are three basic steps to be dealt with, represented in table 1.12, table 1.13 and table 1.14;

1. Review Operational Readiness;

<table>
<thead>
<tr>
<th>Description</th>
<th>Many times when a system transitions to a production environment, unplanned modifications to the system occur. If changes are significant, a modified test of security controls, such as configurations, may be needed to ensure the integrity of the security controls.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Outputs</td>
<td>Evaluation of security implications due to any system changes.</td>
</tr>
<tr>
<td>Synchronization</td>
<td>• System Administrator and ISSO confirmation to System Owner that system is operating normally and compliant with security requirements. • Should a last minute change occur that fundamentally changes the level of risk to the system, the system owner should consider recertification - this is rare.</td>
</tr>
</tbody>
</table>

Table 0.10: Review Operational Readiness

2. Perform Configuration Management and Control;

<table>
<thead>
<tr>
<th>Description</th>
<th>Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently for controlling and maintaining</th>
</tr>
</thead>
</table>
an accurate inventory of any changes to the system. Changes to the hardware, software, or firmware of a system can have a significant security impact. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

| Expected Outputs | • Change Control Board (CCB) decisions  
|                  | • Updated security documentation  
|                  | • Security evaluations of documented system changes. |
| Synchronization  | • System updates should be included into the system security documentation at least annually or with significant change.  
|                  | • CM system documents should provide input into the Continuous Monitoring plan for the system. |

Table 0.11: Perform Configuration Management and Control

3. Conduct Continuous Monitoring;

| Description | The ultimate objective of continuous monitoring is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates. A well-designed and well-managed continuous monitoring process can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. This information can be used to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the continued operation of the information system and the explicit acceptance of risk that results |
The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits. Automation should be leveraged where possible to reduce level of effort and ensure repeatability.

<table>
<thead>
<tr>
<th>Expected Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Documented results of continuous monitoring</td>
</tr>
<tr>
<td>• Security reviews, metrics, measures, and trend analysis</td>
</tr>
<tr>
<td>• Updated security documentation and security reaccreditation decision, as necessary</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous monitoring should be adjusted as risk levels fluctuate significantly and security controls are modified, added, and discontinued.</td>
</tr>
</tbody>
</table>

Table 0.12: Conduct Continuous Monitoring

Stage 5: Disposal:

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

Key security activities for this phase include:

- Build and Execute a Disposal;
- Archive of critical information;
- Disposal of hardware and software.

The three basic steps listed above are what mark the end to the properly planned and listed SDLC; table 1.15, table 1.16 and table 1.17 summarize this.
1. Build and Execute a Disposal;

| Description | Much like a work plan, this plan identifies necessary steps, decisions, and milestones needed to properly close down, transition, or migrate a system or its information. In many cases, disposed systems or system components have remained dormant but still connected to the infrastructure. As a result, these components are often overlooked, unaccounted for, or maintained at suboptimal security protection levels thus, providing additional and unnecessary risk to the infrastructure and all connected systems. A transition plan assists in mitigating these possible outcomes. |
| Expected Outputs | Documented disposal plan for closing or transitioning the system and its information. |
| Synchronization | Security documentation should reflect pending plans if security decisions and funding are reallocated or otherwise impacted because of the disposal decision. |

Table 0.13: Build and Execute a Disposal

1. Ensure Information Preservation;

| Description | When preserving information, organizations should consider the methods that will be required for retrieving information in the future. The technology used to retrieve the records may not be readily available in the future (particularly if encrypted). Legal requirements for records retention must be considered when disposing of systems. |
| Expected Outputs | Index of preserved information, and its location and retention attributes. |
| Synchronization | Records management and Privacy Act requirements should be considered. |

Table 0.14: Ensure Information Preservation
2. Dispose of Hardware and Software;

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and software can be sold, given away, or discarded as provided by applicable law or regulation. The disposal of software should comply with license or other agreements with the developer and with government regulations. There is rarely a need to destroy hardware except for some storage media that contains sensitive information and that cannot be sanitized without destruction. In situations when the storage media cannot be sanitized appropriately, removal and physical destruction of the media may be possible so that the remaining hardware may be sold or given away. Some systems may contain sensitive information after the storage media is removed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expected Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disposition records for hardware and software. These records may include lists of hardware and software released (sold, discarded, or donated), and lists of hardware and software redeployed to other projects or tasks within the organization.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updating of system and component inventories.</td>
</tr>
</tbody>
</table>

Table 0.15: Dispose of Hardware and Software

1.4 Technical Best Practices for Handling Violations to Confidentiality, Integrity, Availability, and Accountability

Previous sections discussed general processes for secure systems. This section discusses technical best practices that can be used to enforce confidentiality, integrity, accountability, and availability policies. Information transferred in the Smart Grid systems could be manipulated by an attacker to affect grid reliability or cause large financial impacts to both utilities and energy consumers. For example, if an attack could successfully modify price information or meter information, customers’ energy bills could be affected. Also, a customer could deny receiving some information which will result in a dispute between participants of the system or decrease in customer’s confidence. To protect information from any kind of attacks, such as eavesdropping, Man-in-the-Middle (MITM) attacks, and unauthorized access or modification of information, cryptographic schemes, such as Symmetric and Asymmetric algorithms, can be used to provide security goals – Confidentiality, Integrity, Availability and Accountability.
Several authentication techniques can be used to ensure the identities of the users in the system. Also, access control policies can be used to provide authorization or privilege.

**Use of Cryptographic tools**

**Confidentiality**

If an attack can gain some customer information, such as energy usage or other personal information, the privacy of the customers will be invaded. Also, some critical information like Demand Response strategies could not be accessed or known by an adversary, since he can manipulate the information to extend some knowledge of the system and use that information to attack the system.

To provide confidentiality of the information, encryption techniques can be used. One of them is to use symmetric or shared key method. The information can be encrypted and decrypted by using shared secret key which is usually known by both sender and receiver. Thus, even if an attacker intercepts the information transmitted between the components in the system, the plaintext will not be discovered without the knowledge of the secret key. However, this approach has major flaws. One of them is that, in practice, the shared key may be distributed to more than two entities and hence it increases the chance for leaking of the key. Also, if the key is compromised, all the communication using that key will be no longer secure. Moreover, the key distribution is extremely expensive and difficult to manage because every entity in the system must have shared keys to communicate with others.

Another approach is to use public key encryption to provide confidentiality of the information. This technique requires each entity has a pair of keys – Public and Private Keys. Public key usually is known by public, but private key is known by only its owner and will not be disclosed to anyone. Only the key pair can be successfully used to encrypt and decrypt the message. Even though these keys go in pairs, it is extremely difficult to derive one from the other. To encrypt the plaintext, the sender will use the public key of the recipient. Hence, the receiver will use his own private key to decrypt the cipher text. The figure 1.2 describes how to provide encryption and decryption using public key.
The public key encryption provides higher security level than secret key encryption because the private key will not be distributed to others and the only one who can decrypt the message is the owner of the private key. On the other hand, the computation of the asymmetric approach is more complex than of the symmetric approach since the key size and ciphertext are much larger, so the performance of the system may be slower than using symmetric cryptography.

Additionally, in some system, the information can be real-time based, which the performance of the system must be of concern. Using asymmetric approach may not appropriate. Another approach is to combine the use of symmetric and asymmetric cryptography. The public key can be used as a long-term key, while the shared key is used as temporarily (or session) key. Before the communication takes place, both sender and receiver can exchange the session key by using the other end side’s public key to encrypt the shared key. After the shared key is established, both sender and receiver use the shared key to encrypt and decrypt data for the communication. When the communication is ended, shared key may be re-used or established again. This way the communication will not be delayed because of the size of the message and be secured since the session key will be used as a short-term key or one-time key.

**Integrity**

---

The term integrity can be used to refer to both source integrity (authentication) and data integrity (message integrity). If an identity of source is not verified, an attacker can inject false message into the system or the message can be come from fraudulent source. Also, if the information sent in the system is modified, the system must be able to detect the modification has been made. The impacts of the breach in this security goal are varied from the grid itself to customers’ billings. Man-in-the-Middle (MITM) attacks or other forms of unauthorized modification attack can be carried out, if the system fails to provide defensive mechanisms against those kinds of attack.

In the symmetric approach, identities of both the sender and receiver are authenticated because only the sender and receiver know the shared key. Therefore, in some cases, the use of shared key technique also provides source integrity. Message authentication can be provided using Message Authentication Code (MAC). MAC is authentication tag which is generated by applying MAC algorithm together with shared secret key and the message. MAC can be computed and verified by using the same key. Thus, the receiver uses the same shared key of the sender to verify if the message is modified or not. MAC algorithm can be done using Hash function. The figure 1.3 demonstrates the use of MAC for message authentication. The notation K in the figure referred to shared key between the sender and receiver.

![Figure 0.2: Message Authentication Code](image)

Thus, when the receiver can verify if the message has been modified by using the same MAC algorithm and shared key to compute MAC from the receiving message and compare it with the

---

MAC part of the receiving message. If they are equivalent, the receiver can be ensured that the message has not been modified.

Another way to provide integrity is to use asymmetric approach. In public key scheme, Digital Signature Algorithm (DSA) can be used to provide authentication and message integrity. Digital Signature is analogous to hand-written signature. However, it is very difficult to be counterfeited because it can combine the name and identity of the signer. The signature part is generated by using Secure Hash Function and the sender’s private key. The sender encrypts the hash of the original message using his private key. When the message is received, the recipient verifies that the message has not been altered in transit using public key of the sender and the same hash function. The source of the message is authenticated, because only the corresponding public key can verify the signature. Thus, Digital Signature provides both source and data integrity. The figure 1.4 below shows the process of signature generation and verification.

![Signature Generation and Verification](image)

Figure 0.3: Signature Generation and Verification

One issue with the use of public key cryptography is that the public key must be certified. That is, one has to prove that it belongs to the intended user and is not a forged. For example, an adversary uses a public key with the name and identity of the intended recipient instead and uses this bogus key to communicate with the system. Digital Certificate can be used to ensure that the public key is authenticated and come from the source that it claims.

Typically, Digital Certificate contains a public key, the certificate information regarding the public key and the digital signature of a Certificate Authority (CA). The certificate information

---

can be the name and identity of the public key or subject data, the algorithm used and date range which is considered valid of the certificate. The signature part of the certificate is derived from a public key and the credential of the public key owner and digitally signed with CA’s private key. The recipient of the certificate uses CA’s public key to verify the certificate. CA can be an internal or external organization or a trusted third party who can certify the public key associated with the name and identity of the owner. Thus, the use of certificate ensures that the public key in the certificate belongs to the owner or subject of the certificate.

Availability

Availability of data is to have data available in a timely manner. In the Smart Grid system, some information, such as Real-Time Pricing (RTP) information and Demand Response events, is required to be accurate and available all the time. However, an attacker can perform Denial of Service attacks (DoS) which usually affect the availability of the system. Mutual authentication techniques could be used to reduce the number of DoS attacks since both client and server must authenticate each other before the communication takes place. However, an attacker still can flood the network with large amount of packets in order to exhaust the bandwidth limits, resulting in loss of availability. Therefore, cryptographic approaches alone are not enough to defend against DoS attacks. Other security measures, such as using Intrusion Detection System (IDS) and Firewall with Access Control list, applying secure software development methodology, using secure communication protocols, should be applied. Legacy devices at end user and low bandwidth of communication channels may result in the loss of availability as well.

Accountability (Non-repudiation)

When a user receives some information, such as price information, and performs some response based on the energy price received, there may be a risk that the user can deny receiving the information. Thus, the mechanisms for checking to see if the system already sent the information to the user and/or the user already received the information are necessary. The system must provide the means to ensure that the user is accountable for his or her action. The failure to provide accountability may result in a dispute between a user and the system provider and also decrease the customer’s confidence.

Digital signature technique can be used to provide accountability. Typically, a private key is only known by the owner and restricted from public. When a user receives the information with is digitally signed using DSA, only the corresponding public key can ensure that the sender is the only one who signed the message. This could prevent the sender from successfully denying that he or she sent the information.

On the other hand, to prevent the receiver from deny receipt of the information, the response message which has to be signed by using the private key of the receiver is needed. The response message should include all the contents of the information received, plus the identity of the receiver, along with the signature part. The signature part is generated by using the private key of the receiver, the identity of the receiver and the secure hash function. Because the response message is digitally signed with the private key of the receiver, therefore only the
corresponding public key can ensure the receiver is the only one who can sign the message. This can ensure that receiver is held accountable for receiving the information.

To implement this technique in Smart Grid system, there must be some secure storage to keep the digital signatures of both sender and receiver. When a disputation takes place, the digital signatures stored in the storage can be used to verify accountability.

**User Authentication**
Before a user can gain access to any resources, such as files, processes, or data, of the system, the identity of the user must be successfully verified and the user must have the right to access those resources. The process of verification of the user’s identity is called user authentication. After the user is authenticated, access control mechanisms can be used to check to see if the user is allowed to access the required resource. The detail of access control will be discussed later in this section.

Authentication can achieve in many ways, such as using password, biometric and public key cryptography, thus choosing the appropriate method is one of the crucial decisions in designing a system. This section is intended to provide commonly use authentication techniques.

**Password Authentication**
Passwords are the most widely used method for user authentication. In general, a user provides the identity and types some word, phrase or password he knows. The system compares the saved password with the received password for authenticating the user. Even though, this method is simple and easy to be implemented, there are vulnerabilities, which need to be addressed.

1. Password may be easy to guess, if the system does not provide security policies for creating user passwords, such as policies against using short passwords or common passwords that are easy to guess.

2. Password must be protected using encryption techniques and stored in secure storage.

3. Countermeasures for password attacks, such as password sniffing and password guessing attack must be provided in order to reduce the risk of discovering password by an attacker.

**Token Authentication**
Token authentication attempts to use something that a user has, such as smart cards, magnetic stripe cards, memory card, cell phones, security tokens, etc., to authenticate with the system. This technique alone may not be secure enough for the system since the token can be stolen and used by an adversary. However, it can be combined with the password or PIN, which provides significantly greater security than using password alone. The use of token and PIN is called two-factor authentication.
**Biometric Authentication**

Biometric Authentication is the verification of an individual based on unique, physical characteristics, such as fingerprint, retina, iris patterns, voiceprint and signature. Biometric authentication provides higher level of security than password authentication, but it is technically complex and expensive compared to password authentication. However, the major advantage of using biometric is that it is not easily stolen or lost. However, to apply biometric method, types of biometrics have to be considered since they have advantages and disadvantages over the others. For example, voice patterns can be easily faked by using a recorder, but it can provide a way to identify the subject without the subject’s knowledge. Fingerprints may be unique and easy to implement, but the subject’s finger needs to be clean, so it may not appropriate to apply to industrial applications.

**Digital Signature**

There may be some case where it is not necessary to authenticate the communicating parties. For example, when downloading music or software patch from the Internet, the server does not need to identify who is downloading, but may have to ensure the users that the data is genuine and is not tampered by malicious software like virus or spyware.

**Access Control/Authorization**

Authorization refers to the act of granting a user or device proper right to access some particular resource of the system. This assumes that the use is already authenticated. To provide authorization, access control mechanisms are necessary. For this reason, the two terms are sometime used interchangeably. Access control is used to prevent unauthorized use of a resource, such as viewing and modifying a resource, including use of resource in an unauthorized manner. The use of access control and encryption will provide confidentiality. Three most commonly used access control policies are Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-based Access Control (RBAC).

**Discretionary Access Control (DAC)**

DAC is based on the identity of the subject, which can be a user, process or component, and on the access rules. The access rules are used to determine whether the subjects are allowed to perform. Access decisions are based on the credentials that the subject presented at the time it is correctly identified, such as username/password, biometrics, and cryptographic tokens. Typically, in DAC model, a subject may have an access right which allows enabling another subject to access to the same resource at the subject’s discretion.

**Mandatory Access Control (MAC)**

MAC is an access policy used in multiple-level systems that require highly sensitive data, such as classified military or government information. MAC ensures the enforcement of security policies by assigning labels on the information and comparing it to the level of sensitivity a subject has. A subject can only access to the data on which it has a label. Additionally, unlike DAC, it is possible for a user to delegate access right to someone else.
Role-based Access Control (RBAC)

RBAC is based on the roles or responsibilities that a subject has within the system and on rules which determine what accesses are permitted for the subject in a given role. Typically, the process of defining roles is based on security policies derived from analyzing fundamental goals and structure of the organization.

Access Control and Smart Grid Communication

Smart grid systems consist of different types of networks, such as Enterprise Bus, Wide Area Network (WAN), Field Area Network, etc. These networks may be implemented using public networks, such as Internet, and non-public network. The communication may go through both public and non-public networks. Thus, an appropriate access control is required to maintain the security requirements. For example, the access control for customer to third party providers, or for the utilities to third party providers. However, the access control policies are tailored to the requirements of networking and communication. For instance, Field Area Network that could be used to connect the energy services interface or the meter in the customer domain and the field device in distribution domain must have the access control which specifies what accesses are allowed and which operations can be performed. If the access control is not specified properly, an attacker may gain access to the meter, and he can cause malicious impacts on the customer domain.

Also, each entity in the smart grid systems, such as Advance Meter Infrastructure (AMI), Home Area Network (HAN) or Neighborhood Area Network, is required to have appropriate access control policies in order to restrict the incoming and outgoing connection to the devices within the network. Access Control List (ACL) must be specified at all nodes which connect between NAN and HAN to limit access to the AMI system.

In addition, the access control policies should be specified in the level of applications or devices. For example, utility operator may be able to perform configuration of the meter remotely, while the customer should be able to only view the price information from the meter. The main purpose of access control is to ensure that the resource is only allowed for an intended user or a device and that the user or device is identified. ACL with access rights for each user and device is required. After the ACL is properly specified, security mechanisms should be implemented to enforce ACL to ensure security policies.

1.5 Secure System Design Principles

This section discusses general principles used in designing secure hardware/software systems. These principles can be used in any phase of the secure system life cycle. In general, these design principles of secure system are mostly based on simplicity and restriction. Simplicity refers to ease of use and ease of understanding the system. It relies on the fact that the simpler the system is, the less can go wrong. Restriction is used minimize permission granting to any entity in the system to access to the resources. There are of eight principles discussed as follows:
1. **Least Privilege**: An entity or a subject must be given only the privileges that are necessary for its tasks, but no more. This Principle ensures that even if, an attacker successfully gains access to some part of the system, it will still difficult for it to gain access the rest of the system. Thus, this principle can reduce the impact of a failure when some part of the system is compromised. Also, the security analysis of each entity will be simplified since it only has minimal privileges. This principle can be used in all parts of the smart grid infrastructure.

2. **Fail Safe Defaults**: A failure of the system should not lead to any change in the security state of the system. This principle ensures that even if the system fails, it is still safe. This principle is used to design firewalls. That is, it will deny all the access by default access is granted only to subjects that are permitted.

3. **Economy of Mechanism**: A design should be as simple and small as possible. When the design or security mechanisms are highly complex, it is likely that the vulnerabilities of the system will be increased. Also, when an error occurs, it will be more difficult to detect. Simplicity refers to all aspects, such as design, implementation, specification, operations, etc. Each tool or component should be designed such that it performs a task in as simple way as possible.

4. **Complete Mediation**: All accesses to every entity in the system must be checked to ensure that subjects have a permission to access that entity. This principle ensures that every access to the system will be authorized beforehand. If the permissions of the objects are changed, the update should be systematically done. A perimeter firewall is an example of a network system that can be used to check all accesses to an internet.

5. **Open Design**: Security cannot rely on obscurity of its design or implementation. The security may be enhanced by the secrecy of design and implementation, but if the design is exposed, the security must not be affected. However, this does not mean that source codes of the programs, cryptographic keys, or any secret information of the programs should be published. Nevertheless, publication of source code can help enhance security because the system can be tested by a wider audience allowing vulnerabilities to be fixed.

6. **Separation of Privilege**: System should not grant the privilege based on single condition. This principle is used to ensure that multiple conditions are met before granting the access to any resources. For example an additional internal firewall is needed for a critical component even if an external perimeter firewall is used for an entire system. Thus, even if an attacker gains one condition, he should not be able to gain permission to any entity. This principle is also known as defense in depth. It is used in several other situations such as multi factor authentication. Authentication can be done using various techniques, some include the physical presence such as Retina scan, fingerprint
detection etc, whereas the other authentication is using through technically sound methods such as password protection.

7. **Least Common Mechanism**: Multiple subjects should not share mechanisms for access to any entity or resource of the system is an unauthorized manner. This principle minimizes the dangers of sharing state among different processes and programs. Thus, every shared mechanism must be designed in such a way that there is no unintentionally compromising security by another. This principle is the reason why isolation is used to ensure security. For instance a ‘honeynet’ can be used to attract attackers so that their modus operandi can be determined. It is important to use this principle to ensure that an attacker does not use the honeynet to attack a production network.

8. **Psychological Acceptability**: A security mechanism should not introduce complexity of accessing the system. This principle is based on a human interacting with the system. The more complex interfaces the system has, the more mistakes the user can make. The designer should ensure that the human interfaces are designed for ease of use so that the users can apply or define security rules without misunderstanding. Also, the installation and configuration of the program should not be complex and when error occurs, the error messages should be easy to understand. This is the principle that should be used for password management. For instance if users are forced to choose very difficult passwords, change it too often, etc. They might find it unacceptable and either write recycle or choose/simpler ones. This principle employee concerns should be heeded.

### 1.6 Conclusion

This chapter discussed general best practices that can be used in securing systems. Applications of these principles to smart grid are mentioned where necessary. The best practices discussed involved all facets of a typical system: people, processes, and technology. The rest of this document discusses best practices for securing important components of the smart grid system using some of the principles discussed in this chapter. The best practices for securing the important smart grid components, namely Demand Response, Customer Domain Systems (i.e. Home Area Networks, Gateways, and Neighborhood Area Networks), Advance Metering Infrastructure, Grid (Supervisory Control and Data Acquisition and Distributed Network Protocol), Plug in Electric Vehicles, and Distributed Energy Resources (DER) are discussed in Chapters 2 through 7 respectively.
CHAPTER 2: 
Demand Response Practices

2.1 Introduction

Demand Response (DR) systems are expected to be eventually utilized in most residential and commercial energy consumers. The security and privacy of customer information must be the highest priority. Proper data handling practices must be carried out in order to protect the security and privacy of customer information. The breach in security goals – confidentiality, integrity, availability, accountability – could adversely affect large scale of a smart grid system and large number of customers. The impacts are varied from the reliability of the grid itself to the financial impacts on utilities and customers as well as the invasion of the privacy of customer information. Consequently, it is important that security concerns and countermeasures are considered at the early stage. This section describes the security concerns in DR and DR network architecture like Sensor Networks. Also, it proposes security measures to defend against possible attacks based on the security concerns specified in this report. Finally, it provides best practices for security purposes related to the DR and Open Automated Demand Response (OpenADR) contexts.

2.2 Demand Response Security Concerns

This section is an overview of the security concerns on the major pieces of the information transmitted in DR systems included pricing signal, DR events information and bidding information.

2.2.1 Pricing Signal

The pricing signal consists of real-time pricing (RTP) and time-of-use pricing (ToU). Real-time pricing requires computer-based response, while the fixed time-of-use pricing may be either manually handled by the customer or automatically handled by the smart device based upon the time periods and the prices.

- **Real-time price** is the electricity prices that fluctuate during different time periods over the course of the day. This dynamic pricing allows customers (industrial, commercial and residential) to shift or shed electricity usage in order to minimize electricity and operating costs for their business. This price signal will show the current price for power and an automation system, such as smart clients or meters, will determine what actions need to be taken based on the pricing signal it received.

- **Time-of-use price** is the electricity prices that are not real-time. This pricing information is defined ahead of time, usually for 24 hour day, and fixed in the certain time periods based on seasons. For example, weekday afternoon in the summer the price is usually on-peak and weekend night during the winter the price is usually off-peak.

Since the real-time pricing information could be daily transmitted via the Internet, it has more security concerns than that of the fixed pricing. The integrity of the price information is of the
most concern. The real-time price could be modified by an attacker in such a way that it affects the organization or customers financially. The modification of the price signals could affect the reliability of the grid. For example, if an attacker modifies the actual price information to be lower than the normal price, the building automation system may shift the electric loads and the blackouts may occur. The automation system at customers’ point must be able to authenticate that the price signals it received is actually come from the utility and not modified by an unauthorized entity. Moreover, confidentiality should be an issue. Eavesdropping on this information, especially the response information that customers make according to the power price, could reveal the electrical usage and invade the privacy of the customer. The customer also may deny receiving price signal or refuse to hold for his action in the response to the price signal. Thus, non-repudiation mechanism needs to be provided. Also, when it comes to real-time based services, the availability of the price information in timely manner could be issue as well.

The fixed time-of-use pricing is less concerned about the confidentiality and integrity of information, since the information is fixed for a certain period of time and is not regularly sent electronically. Thus, the meter reading and the accuracy of data should be only two concerns for ToU pricing.

2.2.2 DR Events Information

DR strategies are pre-programmed in Energy Management Control System (EMCS) at the customers’ sites. The strategies are carried out when the DR events and pricing signal arrives. The main purpose of the DR strategies is to control the electric loads at the end users according to the electric demands in return for decreasing electric usage at end points and providing reliability to the grid. However, if DR events information is manipulated by an attacker by controlling the electricity usage, such as turning on/off the air condition or heating units at end users, this could affect both the utility and participants in DR program financially. Moreover, if an attacker turns on all air conditioning or heating units in a large commercial area, the excessive loads in the grid could occur, leading to blackouts and large financial impacts. In some case, the manipulation of DR events may affect health and safety of customers. For example, an attacker may turn on heating units during an extremely hot day in the summer. This type of attacks can be carried out by Man-in-the-middle (MITM) attacks.

An attacker may attempt to prevent EMCS at customers’ sites from receiving the DR event signals from the utility gateway so that the EMCS cannot shed or shift electric loads. This type of attacks can be carried out by Denial of Service attacks.

The DR events information must be protected from any kind of unauthorized modification and the clients or EMCS must be able to authenticate that the DR signals are come from the legitimate source.

2.2.3 Bidding Information

DR supports several bidding-based programs, such as Capacity Bidding Program (CBP) and Demand Bidding Program (DBP), which are offered through a utility, such as PG&E. Customers, who participate in these bidding programs, can submit a bid for load reduction for
a purposed level of curtailment or against the energy generation resource. In return, the customer will get incentive payment, if the bid is cleared and he reduces the energy consumption according to the bid. The details of how each bidding program works are not in the scope of this paper.

The bidding process begins with the request for a bid from electricity generator, which could be sent in the form of an email, SMS, or by webpage. The customer submits request a bid to the generator. If the bid is accepted, the notification message will be sent to the customer via email, SMS or webpage. However, an attacker can also make a request for a bid or send notification messages by spoofing emails or SMS messages to the customer himself. Also, an attacker could manipulate the load reduction per time block information sent by the customer, causing false behavior of bidding program and financial impacts on bidding participants. For example, an attack pretends to be a customer and issues bidding message instead. Eavesdropping on the load reduction per time block information sent by customers could disclose the energy usage of the customer as well.

2.3 Demand Response Network Architecture

This section is to review some of the network architecture used in DR systems and analyze security concerns in the DR sensor network. Also, it provides security measures to the security concerns specified in this section.

Figure 2.1 describes the high level Demand Response Network Architecture.

![Figure 2.1: Subsystems & Networks in a Sensor Network Based DR Architecture](http://www.law.berkeley.edu/files/demand_response_CEC.pdf)

---

2.3.1 Subsystems and networks in Demand Response Sensor Networks

Demand Response sensor network consists of the followings:

- Sensor clusters or sensor network is a collection of sensors and actuators at either a residence, commercial or industrial building that has the ability to monitor and respond to physical or natural conditions. The communication of each sensor node is based on wireless communications and can be used to receive DR and price signals and send relevant information, such as energy usage or sensor status. However, it has a limited set of computational tasks, including local data aggregation and encoding.

- Cluster gateway node acts as the proxy for each sensor cluster.

- The home or building control subsystem consists of one or more building gateway nodes, sensors and enterprise monitoring & control subsystems. The building gateway node can have scalable LAN/WAN connectivity includes:
  - Wired network such as DSL, Cable, Leased line or Passive Optical Networks (PONs)
  - Wireless network such as cellular network (2, 2.5, 3, 4G) operating in licensed frequency bands IEEE 802.11x networks as well as Mesh networks.
  - Backhaul Networks can be private enterprise networks, such as leased lines, WAN, or public Internet.
  - Other networks, such as SCADA networks.

2.3.2 Sensor Networks and Security Concerns

Sensors have the capabilities of observing information, such as temperature, lighting and humidity and forwarding a response based on the information received to EMCS. For example, in the area that has comfort temperature, air conditioning units may be turned down. Pricing signals can be specified based on sensor data a utility receives as well. However, an attacker may inject some sensor data or disrupt sensor reading which can cause false sensor reading and an inappropriate response to EMCS. Also, some malicious command, such as turning on heating units during the summer, could be inserted into the sensor nodes. This can affect billings and/or health concerns of the customers. The limitation of sensor nodes, such as slow CPUs, short battery life and small memories, should be a concern as well. In order to provide security goals, advanced cryptographic tools must be used; however, complex computations may shorten the battery life and may be slow due to the limited CPUs and memories. The limitation in battery life of the sensor nodes exposes another attack that tries to drain power of sensor nodes by sending a number of messages to them since they have to authenticate and verify each message. Thus, the sensor nodes must not perform much computation on the collected data in order to prolong the battery life. Also, physical attack to a sensor node could make an attacker obtain the keys embedded inside.

2.3.3 Sensor Networks and Security Measures

This section provides security measures in order to defense against the attacks specified in 2.3.2.
Use of Cryptography

If an adversary can capture one or more packets and analyze traffic, he may inject false messages or modify the contents. The system must have the ability to prove that a message comes from the source that it claims and the message has not modified in an unauthorized manner. Many cryptographic approaches could be used to provide particular security goals. One of them is to use symmetric key (shared key) approaches and separate shared keys for each pair of nodes. The node can only communicate with its pair because it requires the same key to encrypt and decrypt the message. Thus, both receiver and sender node can authenticate each other because they have the same shared key. If one of the nodes is compromised, an attacker cannot impersonate the other pair nodes since each pair of nodes requires one shared secret key. To implement this approach, the key has to be distributed ahead of time. Kerberos can be used for the key management and distribution. Data confidentiality is achieved by encrypting the message with the shared key. However, this approach may not be able to support non-repudiation. It also has high communication and implementation costs. Moreover, the battery life for this approach should be of concern since it can be shorter than it is expected to be. This leads to more attractive approach which can be used for sensor-class nodes.

Overview of Elliptic-Curve Cryptography (ECC)

Since sensor networks have the resource limitations, ECC can be an attractive approach which offers the same capabilities of cryptographic schemes used in the Internet communications, such as Digital Signature Algorithm (DSA) and Diffie-Hellman (DH) algorithm, but with the smaller key size. According to RSA Laboratories⁹, Rivest, Shamir & Adleman Public Key cryptography (RSA) with 1024-bit key provide equivalent security level to ECC with 160-bit key. However, RSA laboratories recommend using RSA with 2048-bit key which is equivalent to ECC with 224-bit key to protect data beyond the year 2010¹⁰. ECC also offers Elliptic-Curve Digital Signature algorithm (ECCDSA) and Elliptic-Curve Diffie-Hellman (ECCDH) key exchange which makes it possible to provide mutual authentication, key exchange and ECC-based digital signature for Wireless Sensor Networks (WSN).

Use of ECC in Sensor Network

Authentication

Each sensor node must be able to detect that a message comes from an alleged source and the message has not been modified in an unauthorized manner. Mutual authentication approach can be used to provide such detection. Each sensor node can have its own public and private key pair. According to A. S. Wander¹¹, an abbreviated X.509 certificate can be imitated by

---


¹¹ A. S. Wander; University of California at Santa Cruz, N. Gura, H. Eberle, V. Gupta, S. Chang, C. Shantz; Sun Microsystems Laboratories “Energy Analysis of Public-Key Cryptography for Wireless Sensor
having a unique node identity along with a public key and a signature. Hence, the ECC-based
Secure Socket Layer protocol (SSL) can be implemented. Also, since ECC is based on Public Key
Cryptography, the only phase that affects when applying ECC to SSL is the handshake phase.
Figure 2.2 demonstrates the exchange of message between the client and the server during the
SSL handshake with mutual authentication for both RSA-based and the ECC-based SSL. The
brackets [RSA, ECC] in the figure denote the size of the message in bytes for each algorithm.
The notation C means the client and S means the server.

![Figure 2.2: Simplified RSA-Based and ECC-Based SSL Handshake with Mutual Authentication.
Pay Load Message Size in Byte [RSA, ECC]12](image)

The programmatic details of the message exchange during the ECC-based SSL handshake
protocol is not in the scope of this document. The steps of the simplified version of ECC-based
SSL handshake involve:

1) The client sends a 32-byte randomly generated number or data to the server.

2) The server replies back with the random data received from the first step along with the
server’s certificate. The server’s certificate contains server’s ECDH public key signed by
Certificate Authority (CA) using ECDSA signature. If client successfully authenticate the
server, the client uses its own ECDH private key and the server public key to perform an
ECDH operation to gain the premaster secret. (Note that for RSA-based algorithm, the
message size is 294 bytes while it is only 118 bytes for ECC-based algorithm)

Networks”, March 2005 [online]. Available:

12 A. S. Wander; University of California at Santa Cruz, N. Gura, H. Eberle, V. Gupta, Sheueling C. Shantz; Sun Microsystems
3) The client sends its own certificate to the server. Also, the server performs an ECDH operation using its own private key and the client public key.

4) The derivation of the master key and session key is unchanged from the RSA-based SSL handshake.

To implement this approach, a base station, which acts as a control center or Certificate Authority (CA), is needed for collecting each node’s public key certificate. This mutual authentication approach can authenticate whenever a new node is set up in a sensor cluster or network. In other word, the public keys of all the nodes are needed to be authenticated. Thus, if an attacker tries to set up his own sensor node to intercept the data sent in the sensor networks, he will need to have a certificate, which is usually protected from an unauthorized access to the data in the certificate storage. However, this approach requires each node to keep its pair node’s certificates on its memory; therefore, the size of the certificate should be of concern. (Note that, according to V. Gupta13, a traditional X.509 RSA-1024 certificate is on the order of 700 bytes long, the simplified certificate is only 262 bytes long and an ECC-160 certificate can be reduced from approximately 530 bytes to 86 bytes) Also, the message authentication can be achieved by using digital signature. The use of digital signature can substantially reduce the impacts from Man-in-the-middle (MITM) attacks. The further detail of ECC Cipher Suits for TLS is specified in RFC 449214

Confidentiality

Once the mutual authentication and key exchange between each pair of nodes are established, the shared key can be used to communicate with its pair node. If one of the pair nodes is compromised, the information sent between the other pairs of the node is not revealed since each pair of nodes have different shared key obtained during the key exchange phase. Also, the shared key should be re-established periodically in order to reduce the risk of an attacker gaining knowledge of the key. However, this means the sensor node needs to keep its pair node’s shared key in its memory. This also can be an issue, since the memory size is limited. (Note that, according to RFC 449215, ECC with 160-bit key requires 282 bytes of data memory)

Accountability (Non-Repudiation)


Non-repudiation can be provided by using the digital signature technique. The detail of how to provide accountability is discussed in the section 1.0.

2.3.4 Demand Response and Home Area Network (HAN)

Demand Response systems highly depend on Advanced Metering Systems which provide real time communication link between electric, gas, and water meters. This has led to architecting Home Area Networks that connect thermostats, load switches and lighting devices. All these smart devices connected to HAN can be set to operate during low cost energy period. Introduction of HAN along with advanced wireless home networking has enabled use of home monitoring devices and home automation. The Zigbee wireless communication can be used in home automation for controlling demand response events. This section provides an overview of Zigbee standard and security issues of using Zigbee in HAN in Demand Response context. Also, it provides security measures against the issues specified in this section. This report does not intend to provide comprehensive details of the Zigbee protocol, but rather to provide enough information to discuss about the security issues and measures in the Demand Response context.

Overview of Zigbee Networking Standard

Zigbee is a low-power wireless networking standard which is built on top of IEEE 802.15.4 standard. It is designed specifically for wireless control and monitoring network and can be used to implement HAN devices and appliances in order to provide automation system in the home. Zigbee enables devices to self-assemble into wireless mesh network – from smart meters to devices in home. Zigbee provide two extra security layers which are built on top of IEEE 802.15.4 standard, where the security features are provided. The layers are network and application security layers. The figure 2.3 shows the Zigbee security layers.
Zigbee is based on 128-bit Advance Encryption Standard (AES) algorithm and the Counter Mode with Cipher Block Chaining Message Authentication Code protocol (CCMP). The 128-bit key, which is recommended by NIST\textsuperscript{17}, is considered relatively strong for AES algorithm. Zigbee supports security services, such as access control and frame integrity in order to provide authorization and data integrity. Also, it defends against replay attacks by comparing the sequential freshness value with the last known value and rejecting the data frame that has been replayed (or has the freshness value that has not been updated).

The cryptographic keys in Zigbee can be categorized into three groups as follows:

- Master Key is a long-term key used to establish symmetric keys (Link keys) between two Zigbee-enabled devices. The master keys are pre-installed in the devices by manufacturers in each device or are sent over-the-air to the devices.


• Link Key is unique session key between each pair of devices. The link keys are used to encrypt and decrypt information transmitted between each two devices in the HAN. Link keys are managed by the application layer.

• Network Key is a 128-bit key shared among all the nodes in the network. The network keys can be regenerated by the trust center or coordinator at different period of intervals. The network key is used by each node in order to join the network. It is used for broadcast communication in the network. When the trust center changes the network key, the old network is used to encrypt the new one and it is distributed throughout the network. Each pair of node can have both link key and network key. In this case, the network key will not be used since the link key is more secure.

Use of Zigbee-based HAN in Demand Response

The use of Zigbee in HAN enables electric consumer and utilities manage energy consumption effectively. For example, during the period of peak electrical demand, AMI system and HAN would work together and shed the load based on the price signal or DR events received by the utility in order to manage the high-load devices, such as changing the thermostat setting of the HVAC system in participating homes. The figure 2.4 demonstrates the high-level view of Zigbee-based HAN.

![Figure 2.4: ZigBee-Based HAN Enabling Demand Response from Utilities Network](http://www.pointview.com/data/2008/05/22/pdf/Bob-Gohn-3024.pdf)

The electric meter serves as the gateway, called Energy Service Portal (ESP), between Zigbee-based HAN and (Neighborhood Area Network) NAN or the utility. The ESP communicates with a variety of Zigbee-based devices, including Programmable Communicating Thermostat (PCT), In-home display, Energy Management Consoles, etc. The devices in HAN can receive

---

pricing signals from the AMI network. Load control events which are typically created by the utility can be displayed in the in-home display and allow the utility to schedule turning off high-load applications, such as air conditioners and pool pumps, of the homeowners to manage energy and provide the reliability of the grid. Homeowners still can choose to opt-in or opt-out the events received based on the energy price during the peak demand.

After the utility sends DR events to the ESP, the events will be forwarded to the devices which are responsible for the signals. For example, load control device, which is responsible for shedding or shifting electric loads in the house, will receive the load control events and re-act based on the received events.

2.3.5 Zigbee and Security Concerns

The most concern in the Zigbee-based HAN network is the process of setting up a new device in the network and how the keys are established at both sides of the devices. When the new device is newly connected to the Zigbee network, the key must be established between the new device and its pair node. The key distribution for each pair of nodes in Zigbee standard can be done by three methods as follows:

- Provisioning or Commissioning is to use out-of-bound mechanism, such as pre-installation key or over-the-air key, to place the key into devices. The pre-install methods are not optimal because of the limitation of the ability to write the key in flash memory of the devices when changing the key. Also, the key is sent over-the-air in plaintext, which is susceptible to one-time eavesdropping attack. One way to help this issue is to ensure that devices are in close proximity.

- Key Transport is to have trust center distribute the keys to the devices. This method requires sending the key itself to the devices. The transportation of the key relies on the satisfactory security practice of the vendors. An attacker may be able to intercept the key, if the security mechanism for transporting the key is not secure enough to protect the key.

- Key Agreement is to have trust center and devices negotiate the keys without transport the key itself. According to [DR - 7]¹⁹, Key Agreement is the most secure method for key establishment between devices in the network. The key agreement is based on Symmetric Key Key Establishment (SKKE) which uses the master keys for distributing the shared secret key. However, the master key itself has the issue of the key distribution as well, since it has to be pre-installed or sent over-the-air.

Also, even though Zigbee supports security services and provide mechanism to defend against some attacks, such as eavesdropping and replay attacks, there is still the framework for exploiting IEEE 802.15.4 and Zigbee, called KillerBee. KillerBee framework is published by Josh

Wright\textsuperscript{20}, Senior Security Analysis at InGuardian Website in October 2009. It can be used to analyze Zigbee security; and could be used for Zigbee exploitation as well. KillerBees can be used for sniffing and injecting packets as well as decoding and manipulating network packets. The result from [DR - 6]\textsuperscript{21} has shown some successful attacks using KillerBee to obtain the key and carry out replay attacks. If an attacker can inject the false message into the HAN network, the response of the device to the DR events or pricing information may be false. This can have financial and/or health-related impacts on homeowners. It also can lead to grid failure. Thus, using Zigbee alone may not be enough to provide security for Demand Response in HANs.

2.3.6 Zigbee and Security Measures

Zigbee protocol is based on symmetric keys; the communication is secured by using shared key. However, the shared secret-key scheme has the issues in that if the key is compromised, all communications between the devices that use the same shared key will be no longer secure. Also, the key distribution is also expensive since Zigbee uses mesh-networking which means any device has to store the secret keys of all of its pair nodes in order to have multiple potential paths to route to their destination. Thus, symmetric algorithms cannot scale to a large system with hundreds of devices. The solution to these is to consider Elliptic-Curve Cryptography (ECC) as a public key scheme for Zigbee. ECC offers Elliptic-Curve Diffie-Hellman (ECCDH) key exchange which could be used for the key agreement method. According to E. Barker\textsuperscript{22}, ECC with 160-bit key provides equivalent encryption as strong as AES algorithm with 128-bit key. Also, authentication and non-repudiation can be provided by ECC as discussed in the section 2.3.3.

2.4 Demand Response Best Practices

To carry out load shed or load shift in buildings or residential areas, energy cost and control signals have to be sent via the Utility Gateway over a network, such as the Internet. When day-ahead and near real-time information arrive to an EMCS through the energy meter or gateway, the electricity demand will be moderated based on the signals received. A Home Area Network (HAN) will be used to distribute energy management information to all HAN devices in the building or home. All of the components used in DR programs, such as smart meters, HAN with DR capabilities, have potential vulnerabilities, once they are deployed on a network. An attacker may inject a malicious command into the system, collect personal information of the


user, or modify the message contents. This section discusses best practices for DR systems in order to provide defend mechanisms against possible attacks specified in this document.

Data Transmission

To ensure integrity of the message, mutual authentication should be used between these devices. The DR and price signals and other information in the DR system also need to be encrypted in order to provide data confidentiality. The appropriate communication protocols for secure communication, such as Transport Layer Security (TLS) protocol, Internet Protocol Security (IPSec), Wireless Fidelity (WiFi) associated with IEEE 802.11i for a wireless local area network (WLAN) and IEEE 802.15.4 using ZigBee with elliptic curve cryptography (ECC) for sensor networks in HAN and NAN, can be used to protect network traffic.

Data handling practices

Information is sometimes sent between utilities and third party contractors, who may perform some kinds of collection of private data. Reusing and disclosing personal data by either utilities or third party could affect the privacy of customer information. Therefore, the information must be controlled in secure manners such that only necessary information of the customer is provided to any data collection entity and only authorized entities can access and use customer information. Also, the utility must obtain individual’s permission prior to using personal information or disclosing private data to a third party. The length of time that a utility may retain customers’ energy usage information must be specified\(^{23}\). There are privacy issues which apply to other parts of the smart grid infrastructure. This will be discussed in more detail in a future document on privacy issues of the smart grid.

Key management

Key management is also critical in DR systems. Not only the information transmitted needs to be protected, but also the key itself needs to be authenticated and protected from the disclosure of the key to public. The use of X.509 public key certificate may provide such a protection.

2.5 Open Automated Demand Response (OpenADR) and Security Measures

This section uses the security concerns addressed in section 2.2 to derive security requirements and to provide some of the best practices based on the security requirements.

2.5.1 Security Requirements

The following set of general security requirements is derived from the security concerns specified in this document:

\(^{23}\) “The length of time that a public utility may or must retain customer usage data or other customer records is not specified in California Public Utility Commission (CPUC) general orders, but has been set at seven years as an internal company policy choice [DR - 1].”
• All of the information transmitted in the OpenADR system must be protected from unauthorized access, inspection and modification from unintended users.
• Information transmitted either to or from the Demand Response Automated Server (DRAS) must maintain confidentiality and integrity from third parties.
• The DRAS must provide accountability for the following transactions
  • Prices received by participants
  • DR events received by participants
  • Bids submitted by participants
• The DRAS must maintain confidentiality of participants, utilities and ISOs.
• The proper access control to the information stored on the DRAS must be provided so that only authorized users can modify it.

2.5.2 Security Measures
The OpenADR communication is based on the Internet and Web Services technologies. Secure communication protocols, such as Transport Layer Security Protocol (TLS), can be used to secure network traffic. According to the Open Automated Demand Response Communications Specification24, the TLS version 1 (or newer) has been chosen. The DRAS interfaces security can be implemented by three approaches as follows:
  • TLS 1.0 with server-side certificates
  • TLS 1.0 with server-side and client-side certificates
  • Web Service Security (WS-Security)

M.A. Piette25 has proposed using the official TLS specification as published by the Internet Engineering Task Force (IETF):
  • 1024-bit Rivest, Samir & Adleman Public Key cryptography (RSA) for key exchange
  • 3DES (Data Encryption Standard) and AES128 (Advance Encryption Standard) for data encryption
  • SHA1 (Secure Hash Algorithm) for Message Integrity Code (MIC)

---


• Hashed MAC (HMAC) for Message Authentication Code.

According to this TLS specification, it is relatively safe and provides high-level integrity. However, TLS itself also has some vulnerability which will be described below. This section analyses those three approaches with respect to security issues mentioned above. (Note that at the time this report is being created, TLS version 1.1 and 1.2 has been released and RSA Laboratories has recommended it to use RSA with 2048-bit key in order to protect data beyond the year 201026)

**TLS 1.0 with server-side certificates**

This is most commonly employed in secure web servers. The server-side certificate is used for one-way authentication that allows clients to know that the web server which is responding to the request is the required one. The major flaw of this method is that the client is not authenticated which is subject to a number of serious Man-in-the-middle (MITM) attacks.

**TLS 1.0 with server-side and client-side certificates**

This approach is similar to the first one, but requires a client to provide its certificate for authentication. Even though, this mutual authentication provides the sense that client must be authenticated before communicating with the HTTPS servers, but the cost to implement this approach is extremely high since every clients' certificates need to be issued and maintained. In addition, there is a problem with TLS standard itself which is subject to MITM attacks related to renegotiation. TLS allows both server and client to request renegotiation of the TLS session at any time. The problem is in order to obtain and validate the client certificate, the HTTPS server need to renegotiate the TLS channel. During the authentication, there is a loss of continuity, which is called “the authentication gap”. The authentication gap bug in the TLS protocol allows an attacker to carry out a number of MITM attacks and inject data into the authenticated SSL communications. This demonstrates that the existing systems which are currently implemented using client certificates authentication are vulnerable. Figure 5.5 demonstrates the process of how an attacker can exploit the defect in TLS.

---

In spite of the face that there is no security-fix currently, to implement OpenADR all the SSL libraries need to be updated with the most recent patches. This vulnerability applies to SSL version 3.0, and all current versions of TLS (version 1.0, 1.1, and 1.2). The short-term fix of this problem is to not allow or disable client-side certificates. However, this approach is intended to be used for more secure channel (which requires both server-side and client-side certificates).

---

Thus, unless this vulnerability is fixed, this approach should not be used because the intended “more” security will not be realized.

**Web Service Security (WS-Security)**

WS-Security is a specification for secure Web Services. It provides approach of how to enforce confidentiality and integrity on Web Services messaging. This standard includes the specification details of how to use Security Assertion Markup Language (SAML), Kerberos and Public Key Infrastructure (PKI) certificate format X.509. This section discusses how to enforce the security goals by using some of the cryptographic tools based on PKI and X.509 certificate format with WS-Security specification.

**Encryption**

PKI supports both the encryption and signing. The use of encryption can be done by using the public key (Asymmetric Cryptography) from the X.509 certificate issued by the CA in order to provide data confidentiality. Figure 2.6 below shows the use of public key encryption.

![Encryption Diagram](image)

**Figure 2.6: Asymmetric Cryptography**

---

However, in the OpenADR system, the information can be real-time based, such as Real-time pricing signal. Using public key encryption could be slow due to the size of ciphertext. Another approach is the combination of both symmetric and asymmetric cryptographies. The public key can be used as a long-term key and symmetric key can be used as a short-term or one-time key. The public key is used to establish a temporary shared secret key between the communication pairs by encrypting the shared key and negotiate with the client. After the shared key is established, both communication pairs use this key to encrypt and decrypt messages.

There are some security issues in providing data confidentiality that need to be addressed.

1) Given the same plaintext, the ciphertext should never be repeated. Randomness can be used to attach with the message, so that the encrypted message will never be repeated.

2) Ciphertext should never be used by an eavesdropper to replay the message. Time stamping can be used to validate that the message is a replay.

3) Encrypted message should never differ in length.

**Source Authentication**

In order to implement authentication with X.509 certificate, Certificate Authority (CA) and Certificate Store are needed. The certificate store is the place where all the X.509 certificates are stored. The X.509 certificates issued by the trusted CA are used to verify that the identity of both the server and client are valid. The certificate includes the credentials, such as the identity and public key, and the signature part which is produced by signing the message with the private key of the CA. When the server received the message, it will use client’s public key obtained from the X.509 certificate to validate the signature. The server ensures that the message came from the claimed source and that the X.509 certificate has not expired.

---

**Message Authentication**

Encryption does not necessarily provide protection from unauthorized modification of the message. Thus, message authentication is needed to provide data integrity. The most commonly used technique is to use Digital Signature Algorithm (DSA) in conjunction with RSA algorithm. Signature is generated by using the sender’s private key and an appropriate Secure Hash Standard (SHS) which should comply with the Digital Signature Standard (DSS), FIPS PUB 186\(^\text{30}\), from the National Institute of Standards and Technology (NIST). The verification process is done by using the corresponding public key of the sender and the same hash function. The receiver of the message can ensure that the message came from the source that it claims and the message is not tempered with by anyone because the only corresponding public key and the same hash function can verify the signature part and only the user that possesses the private key can digitally sign the message. Figure 2.8 demonstrates the process of signing and verification using Digital Signature.

![Diagram of Signing and Verification Process of Digital Signature](image)

**Figure 2.8: The Signing and Verification Process of Digital Signature\(^\text{31}\)**

\(^{30}\) Digital Signature Standard is available at [http://www.itl.nist.gov/fipspubs/fip186.htm](http://www.itl.nist.gov/fipspubs/fip186.htm)

Non-repudiation

Non-repudiation can be provided by using the digital signature technique. Typically, the private key is only known by the owner and restricted from public. Thus, using the corresponding public key can ensure that the sender is the only one who signed the message.

Key Pair Management

The key management is one of the critical parts of OpenADR. A best practice is to use different key pairs for encryption and digital signature since the signatures are used for longer-term authentication and message integrity, but the encryptions are done by using a shorter-term key pair. Also, the key distribution, revocation and key backup processes tend to be different based on what the keys are used for. For example, if the encrypted message is stored on hard disk, the archived version of the private key may be needed to decrypt the encrypted message. Nevertheless, the key pair for digital signature may not need to be changed. Also, to protect a public and private key pair, the secure place to store the private key is needed and it should be restricted such that only an authorized party can access it. Typically, the private key should not be accessed by or sent to any other party including the CA. The public key is needed to be protected from unauthorized modification as well. The public keys from X.509 certificates are signed by the trusted CA which can provide such the protection.

Certificate Management

Certificate management depends on the type of CAs which can be an internal or external organization. For the external CAs, X.509 certificates can be simply obtained by submitting a certificate signing request (CSR). The public/private key pairs will be generated only for use with the requested certificate. For the internal CAs, the certificate management varies depending on to the organization. However, CSR can be used for obtaining the certificates as well. Figure 2.9 shows the process of a client requesting an X.509 certificate from a CA that processes CSR and the process of a CA issuing an X.509 certificate.
If the integrity of the certificate has been compromised, the CA has to revoke X.509 certificates. The certificate revocation list (CRL) is typically available to the public, so that any recipients of a signed message can verify that the certificate has not been revoked.

**Security Consideration in Implementation of X.509 Certificate with WS-Security**

In OpenADR systems, security concerns are focused on confidentiality and both source and data integrity. X.509 certificates can be used as a binary security tokens with the WS-Security specification defined in [DR - 13] in order to provide confidentiality and integrity of the message. In WS-Security, message integrity can be provided by using XML signature in conjunction with X.509 certificates. Also, to keep SOAP (Simple Object Access Protocol)

---


message confidential, XML encryption also can be used in conjunction with X.509 certificates. Even though, using X.509 certificate can reduce the risks of MITM attacks, the designer should be aware that using digital signature alone may not be sufficient to secure SOAP messages. A replay attack could be carried out, if there is no mechanism to detect it. Time stamp, sequence number or expiration date can be included into the signature part of the message or of the SOAP header for some SOAP extension. The use of WS-Security in conjunction with X.509 certificates provides a great deal of flexibility and high-level of confidentiality and integrity, but it tends to have some impacts on the system performance, such as speed and complex computation.

2.5.3 Demand Response at Residential Sites and Security Concerns

The demand response for residential customers is carried out by using a Programmable Communicating Thermostat (PCT). PCT Communication takes place through a broadcast wireless network, such as sub carrier FM, which allows large number of PCTs to receive the information in a single broadcast transmission. When the DRAS receives the demand response signals from the utility, it will provide the signals to a network operating center (NOC), which is responsible for the broadcast of the signals to PCTs. Broadcast messages, consisting of the price signal, will be sent out to the thermostat in order to update the power consumption at the residential sites. The broadcast messages could be manipulated by an adversary in such a way that they can affect the energy usage in residential areas. For example, an attacker may attempt to turn on all air-conditioning units in the residential site resulting in excessive loads to the grid, and blackouts may occur. Also, an attacker could send false message which is not issued from the broadcast network, causing incorrect response from the PCT and incorrect energy price is set. Figure 2.10 summarizes goals of an adversary, threats, possible attacks and mechanism for each scenario on the PCT systems.

![Path of Attack](image)

**Figure 2.10: Path of Attack in PCT System**

2.5.4 Demand Response at Residential Sites and Security Measures

To defend against the security concerns discussed in the section 2.5.3, the layer of defense has been addressed as shown in Figure 2.11.

![Layers of Defense](image)

Figure 2.11: Defend Mechanisms for PCT Systems

This section focuses on the use of cryptographic approaches to provide defensive mechanisms against the security concerns since they are considered as the main defense against attacks. The further details of business logic, detection and environment layers are in the Reference Design for PCT.

**Cryptographic Approaches**

---


E. W. Gunther\(^{37}\) has recommended using Elliptic Curve Cryptography (ECC), which is based on the asymmetric approaches and consumes low energy. The use of ECC for authentication and confidentiality is already discussed in section 2.3.3.

**Key Distribution**

The challenge in the case of PCT is the key distribution issues. When the PCT devices are manufactured, the unique random number must be place into each PCT. This number will be used in the installation process as well as the transmission of cryptographic key information to the device. The key materials could be embedded into the device. This may lead to the issue of key handling and storage since if the PCT is stolen, the knowledge of the key information might be leaked. One solution to this is to separate critical information, such as the key, so that there must not be any single entity possessing enough information by itself to reconstruct the secret. In the PCT system, the random number could be placed into the thermostat along with an out-of-band communication channel. The out-of-band channel could be a phone number or activation code which the installer of the PCT could obtain it confidentially in order to activate or install the PCT into a residential site.

**Key Management**

Key management for PCT system utilizes a three-tiered hierarchy of keys as shown in the figure 2.12.

---


---
The benefit of the hierarchy is that when the primary key is compromised at some point, the backup key can be used instead. The backup key will never be used and keep in secure storage, if the primary one is not compromised. In this hierarchy, there are two entities which are system owner and system operator.

*System Owner* is the highest level of authority for overseeing and control of the entire PCT system. Any Information transferred from the System Owner to the PCT must go to the System Operator. The system owner possesses two separate public/private key pairs, one primary and one back up keys. The primary keys will be used when the system owner authenticates the public key of the system operator and also when the system owner sends system-wide messages, such as emergency messages.

*System Operator* is the responsible for sending messages to PCTs. A public/private key pair will be used for all PCT communication from system operator to PCTs. In some case, the system operator may possess more than one key pair based on the different operating regions, or service territories.
CHAPTER 3:
Customer Domain – Home Area Network, Gateway, Neighborhood Area Network

3.1 Introduction

The customer domain consists of a Neighborhood Area Network connecting the utility to the smart meter installed in the homes of the consumer, the gateway and finally the Home Area network which connects all the appliances at home. There were several security concerns raised within each of the domains and the respective potential security threats were addressed.

In the following sections we will be discussing best practices to overcome these security loopholes within each area of communication.

![Figure 3.1: Customer Domain which includes WNAN, gateway and HAN](http://www.sensorsmag.com/files/sensor/nodes/2008/1526/Figure2.jpg)

3.2 Neighborhood Area Network

In Smart Grid, wireless neighborhood area network (WNAN) has a role to play in the HOME-to-HOME or HOME-to-GRID communication. The WNAN coverage range extends anywhere from the coverage of wireless local area network (WLAN), to wireless wide area network (WWAN). The potential threats, issues and vulnerabilities associated with the protocols considered for WNAN are briefly summarized below.

3.2.1 IEEE 802.11

Wireless network is available everywhere and the attacker need not be in close proximity to the victim. Management frames are not authenticated hence the attacker can take advantage and redirect the traffic and can also corrupt the ARP tables. DOS attacks are performed by introducing the noise into the network. Without proper employment of encryption techniques, there is a scope for eavesdropping and manipulating.

The following are the observed problems with wireless local area network (WLAN):

---

39 [http://www.sensorsmag.com/files/sensor/nodes/2008/1526/Figure2.jpg](http://www.sensorsmag.com/files/sensor/nodes/2008/1526/Figure2.jpg)
3.2.2 IEEE 802.15.4

Encryption scheme must be used to prevent message recovery. To avoid semantic security violation, unique nonce values are used while encryption. The same nonces are sent in the packet with encrypted data and hence decryption is not dependent on the nonce affecting confidentiality. The ACL table gets cleared in case of power failure thereby resetting the nonce to known values and hence the reuse of nonce is incurred, compromising the security. The inability of ACL tables to support different keying modes like group keying and network shared keying could lead to reply attacks. These replay attacks could result in rejecting packets thereby causing denial of service.

The following are the observed problems with IEEE 802.15.4 protocol\(^4\):

- a) Confidentiality
- b) Loss of ACL State
- c) Key Management Problems
- d) Confidentiality and Integrity Protection
- e) Denial of Service
- f) No Acknowledgment Packet Integrity

3.2.3 IEEE 802.16

Wimax is prone to man-in-the-middle attacks, exposing customers to confidentiality and availability attacks as there is no base station authentication schema. Management frames are not encrypted and hence information about subscribers in the area and also about network characteristics could be obtained but by an attacker. An attacker can also send a series of frames to a node to drain the battery life.

The following are the observed problems with IEEE 802.16 protocol\(^4\):

- a) Authentication
- b) Encryption
- c) Availability
- d) Water Torture Attacks

---

3.3 **Best Practices for WNAN**

3.3.1 IEEE 802.11

The following section describes the recommendations for the security of 802.11 networks:

1) **Media access control (MAC) address filtering**\(^{41}\) would allow us to configure our wireless access points (APs) with the set of MAC addresses for allowed wireless clients.

**Pros:** Helps receive information from authentic sources and prevents unauthorized access.

**Cons:** Does not prevent a hacker from MAC spoofing, increases administrative overheads.

2) **Wi-Fi Protected Access (WPA)**\(^{3}\) has an improved encryption algorithm called Temporal Key Integrity Protocol (TKIP) which uses a unique key for every client and also uses longer keys that are rotated at configurable intervals. WPA also includes an encrypted message integrity check field in the packet to prevent denial-of-service and spoofing attacks.

**Pros:** With the use of WPA2, VPN connections are not required to secure the wireless frames.

3) **IEEE 802.11w-2009**\(^{42}\): The management information is sent in unprotected frames, which cause network disruption by malicious systems that forge disassociation requests that appear to be sent by valid equipment. IEEE 802.11w-2009 is an approved amendment to IEEE 802.11 to increase security of the management frames. The objective of this protocol is to increase the security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection.

3.3.2 IEEE 802.15.4

The following section describes the recommendations for the security of 802.15.4 networks:

1) **MAC address filtering:** This security mechanism is defined with the IEEE 802.15.4 standard and is defined in the Access Control List (ACL) mode. This feature should be enabled to accept the received MAC frames from authorized nodes listed in the ACL for the host device.

2) **Flash memories**\(^{1}\): The loss of ACL entries during power failure or low powered operation could be fixed by saving and storing the nonce\(^{9}\) states in flash memories. But the use of such flash memories incur an additional cost, power consumption and also is slow and energy inefficient.


\(^{9}\) See citation
3) **AES encryption standards**\(^{43}\): Data privacy protection mechanisms based on AES encryption standard should be used to protect the transmitted data.
4) **Source node authentication**\(^{44}\): A concept similar to shared secret key or unique session key that is derived between two entities in order to secure data transmitted between them should be used to implement source node authentication.

### 3.3.3 IEEE 802.16

The following section describes the recommendations for the security of 802.16 networks:

1. **Message Authentication Code (MAC) techniques**\(^{45}\): For vulnerability of management message, message authentication code techniques can be applied during initial ranging. For example, one-key message authentication code (OMAC) may be preferable since it provides replay protection.
2. **Protection against masquerading parties**\(^{46}\): A mutual authentication scheme is necessary, and Extensible Authentication Protocol (EAP), a generic authentication protocol used in wireless networks, is most commonly proposed.
3. **AES-CCM**\(^{47}\): AES in CCM mode constructs a unique nonce during the process of CBC-MAC. AES-CCM also has an advantage that the encryption scheme is also capable to protect authenticated but unencrypted data.

### 3.4 Gateway

The home gateway component is an integral part of the customer domain architecture. Since it connects a varied Standard home area network to a native AMI communication standard, it needs to act as negotiation agent and also it needs to do the function of a translation unit. If the gateway is compromised then it could harm either the utility or the home appliances or at times both. Considering the significance of this component the need to come up with a secure solution is at its prime. We in this document are discussing some of the possible countermeasures to the security problems mentioned below.

### 3.4.1 Best Practices for Gateway

1. **MAC address filtering**: When a new gateway is added to the network it would send out its MAC as identification to the utilities. These MAC addresses have to be entered in the Access Control List (ACL) of all intermediate hubs to prevent the MAC address spoofing. But the downside to this approach is once the valid MAC address is sniffed then it can be used to access the network. To avoid eavesdropping we would require using of an encryption scheme.
2. **Low Power Encryption techniques**\(^{48}\): The use of low power cryptographic schemes like

---


\(^{44}\) Hyung-Joon Kim, IEEE 802.16/WiMax Security, Stevens Institute of Technology, Hoboken, New Jersey

\(^{45}\) P Kitsos, O Koufopavlou, G Selimis and N Sklavos, Low Power Cryptography, VLSI Design Lab, Electrical and Computer Engineering Department, University of Patras.
the Asynchronous VLSI implementations of International Data Encryption Algorithm (IDEA). This approach proves to be the most efficient in terms of power consumptions.

3. **Central Authority for Public Key Infrastructure**: The need of a central certifying authority in such set up cannot be more emphasized. The central authority would not just be a certificate issuing unit, but also a central regulatory board which would control all the software and hardware updates to the critical components of the Smartgrid.

4. **Trusted Platform Module**: In computing, Trusted Platform Module (TPM) is the name of a published specification detailing a secure crypto processor that can store cryptographic keys. The TPM can be used to store the Public and Private Key pairs in the sealed storage.

5. **Virtual Home**: The use of a virtual home is beneficial from the consumer’s perceptive; since gateway incorporates a virtual home set up which would execute all the commands received from the outside world on itself before deploying it on the real environment. This adds a security shield to the home area network, but since operation of this virtual home is vital the software updates and hardware tampering needs to be controlled by the regulatory board.

### 3.5 Home Area Network

Home area network is last link in the chain connecting utility to the customer. Since it resides in such close proximity of the consumer, a security failure would directly affect lives of the end user. The Home Area Network (HAN) protocol considered here is ZigBee and security loopholes within the protocol has been discussed in the document Smart grid cyber security potential threats, vulnerabilities and risks. In the present document we would be considering best practices for Zigbee and suggesting counter measures for the security threats.

**ZigBee**: ZigBee’s protocol stack is structured in layers. The physical and the media access layer are based on the IEEE 802.15.4 standard. IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks. It focuses on low-cost, low-speed ubiquitous communication between devices. The 2 layers on top of this stack is ZigBee specific which is General Operation Framework and the Application layer.

Using of Flash memory: The threat scenario due to power failure can be resolved by storing nonce states in flash memory which incurs additional cost, power consumption and energy inefficient.

Avoiding Counter mode in AES: To overcome fast Denial-Of-Service attack, we can avoid using the counter mode in the AES (Advanced Encryption Standard) and use other modes such as CCM which is counter with CBC-MAC (Cipher Block Chaining Messages Authentication Code).

---


47 Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.
Using Single Access Control List (ACL): There is no support for using the same keys for multiple ACL entries. Since ZigBee allows this there is problem of nonce states being reused. To fix the problem we could create a single ACL entry for a particular key. Before sending, changing the destination address associated with that ACL entry for a message would suffice to fix this issue.

3.5.1 General Best Practices for ZigBee

The following are recommended practices that should be considered when implementing a ZigBee LR-WPAN network:

- **Creating a Security Policy within the organization:** Develop a general LR-WPAN technology security policy and make it part of the existing IT policy would help authorize the use of LR-WPAN networks within the organization and specify the roles and responsibilities of personnel to ensure their safe and secure operation.

- **MAC Address Filtering:** This is the security mechanism defined with the IEEE 802.15.4 standard and is the Access Control List (ACL) mode. This feature should be enabled to accept received MAC frames from authorized nodes listed in the ACL for the device.

- **Encryption:** To protect the transmitted data ZigBee provides data privacy protection mechanism based on AES encryption standard.

- **Source node authentication:** A destination node in a ZigBee network can use a link key derived from their respective master keys to verify the identity of the source device. The link key is unique for a pair of devices that communicate with each other. (This is equivalent to the concept of a unique session key that is derived between two entities in order secure data transmitted between them.)

- **ZigBee Coordinator:** ZigBee coordinator is a node that is responsible for initiating the formation of network, sending the beacon transmissions and setting the security level. Unlike in Bluetooth where there is only one fully functional device (FFD)† and the rest are reduced functional devices (RFD), ZigBee could have more than one fully functional device and hence it becomes important to designate a ZigBee coordinator for the network which owns the responsibility to perform the above mentioned essential functions. It is also advisable to have a backup ZigBee coordinator which comes handy in case of failure.

- **Restrict node connectivity using a pre-assigned PAN Identifier:** If multiple ZigBee networks are operating in a given environment there is a high possibility for conflicts to

---


† See citation
occur. Hence a ZigBee network policy could be employed to use the permit join access control to restrict device connectivity. This is performed in addition to configuring a dedicated ZigBee Coordinator for the network, where in ZigBee nodes should be limited to joining only the network with the pre-assigned PAN Identifier.

- **Out-of-band key loading method:** This is one of the possible key management methods used by ZigBee vendors. In this method the key could be loaded on the device using methods other than the normal wireless communication channels like, via a serial port of the device connected to a key generation device like a laptop or trust center.

- **Secure network admission control:** The secure join method provides a way to authenticate the nodes requesting admission and decide whether or not to permit the node to join the network. This functionality is carried out by a ZigBee Trust Center where in it allows nodes to first associate themselves to a network and then authenticates to it. This is done by pre-loading a common network shared key in the devices before deployment.

- **Trust Center address to be preconfigured in all nodes:** The Trust Center (TC) is the central element in the ZigBee security architecture and is trusted by all devices in the network. The address of the TC should be pre-loaded into the ZigBee node.

- **Interference:** Industrial environments can produce a significant amount of electromagnetic noise from machinery such as pumps, motors, fans, and various actuator devices, thereby reducing the signal-to-noise quality of transmissions in a LR-WPAN network. The MAC layer of 802.15.4 is based on the CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) channel access method in which a station will first listen for an open channel before transmitting. This is done by sensing the energy level in the frequency band corresponding to the channel. The possible solution to over this interference problem include:
  
a. Choosing the least susceptible 802.15.4 frequency band (900MHz or 2.4GHz) for a given industrial environment.
b. Configuring the ZigBee devices to use a particular channel within the selected frequency band that is least affected by the EMI.
c. Increasing the transmit power level of the ZigBee devices by selecting a product that supports higher power levels or using a higher-gain antenna.
d. Deploying a mesh topology to allow a ZigBee device to have multiple next-hop neighbors to communicate with and therefore *spatial diversity* in terms of multiple transmission paths. Higher node density will also permit shorter distances between ZigBee devices and can result in increased received signal strength and improved signal-to-noise ratios.
e. Using a Frequency Hopping (FH) radio with configurable hopping channels and patterns. This type of temporal and frequency diversity approach can improve EMI immunity in an industrial environment as well as provide an additional
measure of security if a non-default hopping pattern is used and also changed on a periodic basis.

## 3.6 Comprehensive Best Practices for Securities with HAN/Gateway/WNAN

<table>
<thead>
<tr>
<th>Component Involved</th>
<th>Threat Scenario Description</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>U-SNAP</td>
<td>MAC address spoofing</td>
<td>MAC address filtering, Low Power Cryptography techniques, Central Authority for Public Key Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Public Key Infrastructure security issues</td>
<td></td>
</tr>
<tr>
<td>ZigBee Gateway Module</td>
<td>External security threats and loopholes</td>
<td>Virtual Home</td>
</tr>
<tr>
<td>ZigBee</td>
<td>Power Failures</td>
<td>Using of Flash memory</td>
</tr>
<tr>
<td></td>
<td>Fast Denial-Of-Service Attack on AES-CTR</td>
<td>Avoiding Counter mode in AES</td>
</tr>
<tr>
<td></td>
<td>Allows the use of Same Keys on multiple ACL entries</td>
<td>Using Single Access Control List (ACL)</td>
</tr>
<tr>
<td>IEEE 802.11</td>
<td>MAC Spoofing</td>
<td>Media access control (MAC) address filtering, Wi-Fi Protected Access (WPA)</td>
</tr>
<tr>
<td></td>
<td>Denial of Service Attacks</td>
<td>IEEE 802.11w-2009</td>
</tr>
<tr>
<td></td>
<td>Man-in-the-Middle Attacks</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.16</td>
<td>Authentication</td>
<td>Message Authentication Code (MAC) techniques</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>Protection against masquerading parties</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
<td>AES-CCM</td>
</tr>
<tr>
<td></td>
<td>Water Torture Attack</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.15.4</td>
<td>Confidentiality</td>
<td>MAC address filtering, AES encryption standards, Flash memories</td>
</tr>
<tr>
<td></td>
<td>Loss of ACL State</td>
<td>AES encryption standards</td>
</tr>
<tr>
<td></td>
<td>Key Management Problems</td>
<td>Source node authentication</td>
</tr>
<tr>
<td></td>
<td>Confidentiality and Integrity</td>
<td></td>
</tr>
<tr>
<td>Component Involved</td>
<td>Threat Scenario Description</td>
<td>Best Practices</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Protection</td>
<td>Denial Of Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No Acknowledgment Packet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.1: Comprehensive Best Practices for Securities with HAN/Gateway/ WNAN
CHAPTER 4: Advanced Metering Infrastructure (AMI)

4.1 Introduction

Advanced Metering Infrastructure (AMI) refers to systems that measure, collect and analyze energy usage, from advanced devices such as electricity meters, gas meters, and/or water meters, through various communication media on request or on a pre-defined schedule. This infrastructure includes hardware, software, communications, customer associated systems and meter data management (MDM) software.\(^49\)

The network between the measurement devices and business systems allows collection and distribution of information to customers, suppliers, utility companies and service providers. This enables these businesses to either participate in, or provide, demand response solutions, products and services. By providing information to customers, the system assists a change in energy usage from their normal consumption patterns, either in response to changes in price or as incentives designed to encourage lower energy usage use at times of peak-demand periods or higher wholesale prices or during periods of low operational systems reliability.

AMI systems are viewed as consisting of the following components (see also Figure 4.1):\(^50\)

- **Smart Meter** – The smart meter is the source of metrological data as well as other energy-related information. These smart meters can provide interval data for customer loads as well as distributed generation.

- **Customer Gateway** – The customer gateway acts as an interface between the AMI network and customer systems and appliances within the customer facilities, such as a Home Area Network (HAN) or Building Management System (BMS). It may or may not co-locate with the smart meter.

- **AMI Communications Network** – This network provides a path for information to flow from the meter to the AMI head end.

- **AMI Head End** – This system manages the information exchanges between external systems, such as the Meter Data Management (MDM) system and the AMI network.

---

\(^49\) Wikipedia; Advanced Metering Infrastructure; Available [Online]: http://en.wikipedia.org/wiki/Advanced_Metering_Infrastructure

\(^50\) Open Smart Grid; Shared Documents; Available [Online]: http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx
4.2 AMI Security Best Practices

Utilities are spending considerable amount of resources to develop Advance Metering Infrastructure systems with future vision that provides operational efficiency by enabling consumers to participate in personal energy management and conservation and also supports smart energy, distribution grids etc.

AMI have several benefits including filed operations, load forecasting, meter management and several areas such as: customer care, power outage management, reducing dependence on nonrenewable 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.

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

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

4.3 Basic AMI Security Considerations

Baseline security requirements can be classified by high-level functionality. These include confidentiality and privacy, integrity, availability, authentication and non-repudiation/accounting. The foundation of much of this functionality is based on cryptographic services including cryptographic key management and cryptographic operations for a number of purposes, including to:

- Cryptographically authenticate metering assets to the network to ensure that only known and approved devices participate in the network
- Authenticate and integrity check system commands, at the meter, to ensure they are authorized and haven’t been tampered
- Guard against replay attacks to prevent denial of service attacks or load shedding and ensure availability of system resources
- Encrypt meter data to protect consumer privacy
- Provide a means of non-repudiation for consumer demand response programs
- Provide integrity protection and origin authentication of meter data.
- Authenticate and integrity check meter firmware and configuration images when updates are provisioned.
- Adopt an open reference standard for security of advanced meters.
- Enforce full implementation of the security standard by advanced meter vendors.
- Authenticate all commands from the head-end to the customer endpoint.
- Authenticate all reporting from the customer endpoint to the head-end.
- Protect head-end systems as if they were critical cyber assets in the sense of NERC CIP-002.
- Implement host-based intrusion detection with software integrity checking of the headend systems.
- Perform frequent, irregularly scheduled audits of head-end outputs to ensure they reflect inputs.

• Use strong user authentication on all head-end systems and log all user actions.

• Implement network separation, strong firewalls, and limited router access control lists in the AMI network.

• Implement strong separation between the AMI network and the electronic security perimeters of other systems such as EMS.

• Implement safety logic to prevent rapid changes in pricing information sent from the head-end to the customer endpoint.

Beyond baseline cryptographic services, systems and processes are also needed to manage assets in a secure fashion. For instance, system keys must be protected from disclosure through physical and policy-based mechanisms. Role based access controls should authenticate utility operations personnel authorized to manage the system and provide a secure audit trail when system management or maintenance tasks, such as updating of keys is performed.

4.3.1 Code Signing and Firmware Authentication

Code signing\(^\text{54}\):

It is a mechanism whereby publishers of software and content can use a certificate-based digital signature to verify their identities to users of the code, thus allowing users to decide whether or not to install it based on whether they trust the publisher. Code signing is based on the use of a digital signature, which is in turn is based on a digital certificate issued by a trusted third party (a certification authority) that has verified the identity of the software or content publisher. When a developer enrolls for a digital ID, he is required to submit documentation of proof of identity. A public/private key pair is generated when the certificate is requested. The private key stays on the requester’s computer and is never sent to the CA. It should not be shared with anyone. The public key is submitted to the CA with the certificate request.

After the certificate is issued, the developer uses the private key associated with that public key to sign his code. When users download the signed code, they get a copy of the certificate verifying the identity of the author/publisher. The Web browser verifies the digital signature, and the user knows that the code did indeed come from that particular developer.

Here is exactly what happens when a developer signs the code:

1. The code is put through a one-way hash function. This creates a “digest” of fixed length.
2. The developer’s private key is used to encrypt this digest.
3. The digest is combined with the certificate and hash algorithm to create a signature block.
4. The signature block is inserted into the portable executable file.

\(^{54}\) http://www.windowssecurity.com/articles/Code-Signing.html
What happens at the other end (on the computer that downloads the signed code)? Here’s the process:

1. The certificate is examined and the developer’s public key is obtained from the CA.
2. The digest is then decrypted with the public key.
3. The same hash algorithm that was used to create the digest is run on the code again, to create a second digest.
4. The second digest is compared to the original.

If the two digests match, you know that the public key is the one that matches the private key used to sign the code, and you know that the code hasn’t been changed since it was signed.

A key step in building a strong security foundation is to establish a root of trust for every device. This enables each device to validate its operating environment, including any modifiable software or configuration files. It is when firmware is being reprogrammed that devices can be most vulnerable. To ensure image code integrity and authenticity, the core boot loader should be stored in protected (read only) memory. Signatures should authenticate firmware and sensitive configuration data. In order for those signatures to be legitimate, OEM authentication keys should also be protected from unauthorized modification – preferably stored in one-time-programmable (OTP) memory. Configuration data should be bound to the device identity, such as a unique MAC address.

### 4.4 Best Practices for the Security Issues

#### 4.4.1 For Customer Threat

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.

#### 4.4.2 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.

To organize the security issues in different areas of AMI, below is the described table for best practices for each of the areas.
4.5 Best Practices for Different Areas of Security

Below are some of the best practices with detail description (Table 4.1 and Table 4.2), which we have used as acronyms in the threat and best practices tables (Table 4.3 through Table 4.15).

<table>
<thead>
<tr>
<th>Objective Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin_Roles_Access</td>
<td>Design administrative functions such that administrative responsibilities of the system will be well defined and compartmentalized such that administrators do not automatically have access to assets, except for necessary exceptions.</td>
</tr>
<tr>
<td>Audit</td>
<td>Record in audit records: date and time of action, location of the action, and the entity responsible for the action.</td>
</tr>
<tr>
<td>Audit_Log_Maintenance</td>
<td>The audit log will be maintained in such a way as to prevent unauthorized access, modification, deletion or overflow conditions.</td>
</tr>
<tr>
<td>Trusted_Path&amp;Channel</td>
<td>Provide a trusted path and channel between the system and a remote trusted system for the performance of security-critical operations.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Provide high assurance that information is not disclosed to unauthorized individuals, processes, or devices.</td>
</tr>
<tr>
<td>Objective Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Crypto_Comm_Channel</td>
<td>Provide secure session establishment between the system and remote systems using NSA approved confidentiality, integrity, authentication and non-repudiation of network transmissions. Restrict user access to cryptographic IT assets in accordance with a specified user access control policy. Provide complete separation between plaintext and encrypted data and between data and keys.</td>
</tr>
<tr>
<td>Crypto_Storage</td>
<td>Provide NSA approved confidentiality, integrity, authentication and non-repudiation of stored information content.</td>
</tr>
<tr>
<td>Crypto_IMPORT_EXPORT</td>
<td>Protect cryptographic data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.</td>
</tr>
<tr>
<td>Import_Export_Control</td>
<td>Provide security services and labels on import/export data that is consistent with policy (i.e. user, data source, data content, and intended audience).</td>
</tr>
<tr>
<td>Fault_Tolerant</td>
<td>Provide fault tolerant operations for critical components and continue to operate in the presence of specific failures in one or more system components.</td>
</tr>
<tr>
<td>Integrity_Checks</td>
<td>Provide periodic integrity checks on system data, user data, and hardware/software functionality.</td>
</tr>
<tr>
<td>I&amp;A</td>
<td>Uniquely identity and robustly authenticate each user that will support accountability and authorization.</td>
</tr>
<tr>
<td>Objective Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Integ_Data</td>
<td>Ensure the integrity of system data, user data, and security attributes transferred or replicated within the system.</td>
</tr>
<tr>
<td>Emanantions</td>
<td>Limit system-produced unintended emanations (intelligible or not) to within a specified limit.</td>
</tr>
<tr>
<td>Isolate_Executables</td>
<td>Run executable code in a protected domain where the code's potential errors or malicious code will not significantly impact other system functions of other valid users of the system.</td>
</tr>
<tr>
<td>Maintain_Online</td>
<td>Provide online maintenance role with a limited capability to observe the usage of specified services or resources as necessary.</td>
</tr>
<tr>
<td>NonRepudiation</td>
<td>Provide accountability and nonrepudiation of information transfer between entities.</td>
</tr>
<tr>
<td>Obj_Attr</td>
<td>Maintain object security attributes with integrity.</td>
</tr>
<tr>
<td>Priority_Of_Service</td>
<td>Control access to resources so that lower-priority activities do not unduly interfere with or delay higher-priority activities.</td>
</tr>
<tr>
<td>Resource_Quotas</td>
<td>Use resource quotas to limit user and service use of system resources to a level that will prevent degradation or denial of service to other critical users and services.</td>
</tr>
<tr>
<td>Rollback</td>
<td>Recover from user operations by undoing some user operations (i.e., “rolling back”) to restore a previous known state.</td>
</tr>
<tr>
<td>Objective Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SW_Download</td>
<td>Provide the ability to update the TOE software program to patch discovered security flaws or other flaws in the program that could be exploited by the adversary. SW download is implemented with High Robustness.</td>
</tr>
<tr>
<td>Session_Protection</td>
<td>Provide protection of a user or admin session to prevent an unauthorized user from using an unattended computer where a valid user has an active session.</td>
</tr>
<tr>
<td>Secure_State</td>
<td>Maintain and recover to a secure state without security compromise after power cycle, addition or removal of components, system error or other interruption of system operation.</td>
</tr>
<tr>
<td>Security_Mgt</td>
<td>Manage the initialization of, limits on, and allowable operations on security attributes, security-critical data, and security mechanisms.</td>
</tr>
<tr>
<td>Security_Roles</td>
<td>Maintain security-relevant roles and the association of users with those roles.</td>
</tr>
<tr>
<td>Sys_Assur_HW/SW/FW</td>
<td>Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.</td>
</tr>
<tr>
<td>Tamper</td>
<td>Provide system features that prevent, detect, and resist physical tampering of a system component, and use those features to limit security breaches.</td>
</tr>
<tr>
<td>Objective Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User_Attributes</td>
<td>Maintain a set of security attributes (which may include group membership, clearance, access rights, etc.) associated with individual users in addition to user identity.</td>
</tr>
<tr>
<td>Secure_via_Cryptography</td>
<td>Ensure the protection provided to data in the system is predicated on the secrecy of the keys not in the secrecy of the design.</td>
</tr>
<tr>
<td>Malicious_Code</td>
<td>Incorporate malicious code prevention procedures and mechanisms.</td>
</tr>
<tr>
<td>Comp_Attributes</td>
<td>Maintain a set of security attributes associated with individual components in addition to component identity.</td>
</tr>
<tr>
<td>Attr_based_Policy</td>
<td>Provide policy based access control via security attributes on Users, Components, and Objects.</td>
</tr>
</tbody>
</table>

Table 4.1: Best Practices for Different Areas of Security
<table>
<thead>
<tr>
<th>Objective Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin_Guidance</td>
<td>Deter administrator errors by providing adequate administrator guidance.</td>
</tr>
<tr>
<td>Config_Management</td>
<td>Implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).</td>
</tr>
<tr>
<td>Crypto_Key_Man</td>
<td>Fully define cryptographic components, functions, and interfaces. Ensure appropriate protection for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.</td>
</tr>
<tr>
<td>Secure_Configuration</td>
<td>Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, in accordance with organizational security policies.</td>
</tr>
<tr>
<td>Evaluated_System</td>
<td>Evaluate system via Common Criteria methods for proper implementation including examination for accidental or deliberate flaws in code made by the developer. The accidental flaws could be lack of engineering detail or bad design. Where the deliberate flaws would include building trapdoors for later entry as an example.</td>
</tr>
<tr>
<td>Sys_Backup_Procs</td>
<td>Provide backup procedures to ensure that the system can be reconstructed.</td>
</tr>
<tr>
<td>Objective Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User_Auth_Management</td>
<td>Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.</td>
</tr>
<tr>
<td>User_Guidance</td>
<td>Provide documentation for the general user.</td>
</tr>
<tr>
<td>Component_Engineering</td>
<td>Manage lifecycle maintenance such that when component hardware becomes obsolete the AMI hardware/software is redesigned to support production</td>
</tr>
<tr>
<td>Admin_Available</td>
<td>Provide at least one Security Administrator (authorized by the U.S. or the host country) to respond to administrative issues including fixing enrollment/I&amp;A issues.</td>
</tr>
<tr>
<td>Trusted_Facility</td>
<td>Provide a trusted facility for initialization.</td>
</tr>
<tr>
<td>Physical_Security</td>
<td>Provide an appropriate level of physical security.</td>
</tr>
<tr>
<td>BackhaulSLA</td>
<td>Negotiate an SLA with the Backhaul network that meets the operational needs of the mission. This includes required fault-tolerant aspects of the Backhaul’s system including but not limited to routers, switch, and even “back-hoe” protection.</td>
</tr>
<tr>
<td>Enrollment_Process</td>
<td>Provide a registration/enrollment procedure that includes both a chain of trust of user identity to enroll (e.g. DoD PKI or a US Passport) plus a chain of trust of access and authorization to those domains to grant access.</td>
</tr>
</tbody>
</table>

Table 4.2: Best Practices for Different Areas of Security
### 4.5.1 Admin Threats

Administrative threats are those threats that are caused by malicious or negligent administrators. These threats are listed below in Table 4.1.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table4.1 and Table4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entity gives access to information assets to inappropriate users</td>
<td>Admin_Roles_Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rollback</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Session_Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security_Mgt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security_Roles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attr_based_Policy</td>
</tr>
<tr>
<td>2</td>
<td>An AMI entity with proper access gives access to resource assets to inappropriate users</td>
<td>Secure_Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User_Auth_Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enrollment_Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>I&amp;A</td>
</tr>
<tr>
<td>3</td>
<td>An AMI entity with proper access gives access to service assets to inappropriate users</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>An AMI entity with proper access enrolls a user with inappropriate levels of access control.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>An entity uses the Lockout service asset in an unauthorized manner to lock out a user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>An entity uses the Lockout service asset in an unauthorized manner to unlock a locked out a user.</td>
<td></td>
</tr>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table 4.1 and Table 4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>---------------------------------</td>
</tr>
</tbody>
</table>
| 7           | An AMI entity with access creates a large policy causing an exhaustion of storage space. | Admin_Roles_Access  
Confidentiality  
Rollback  
Session_Protection |
| 8           | An AMI entity without proper access exploits policy flaws to gain improper (unintended) access to assets. | Security_Mgt  
Security_Roles  
Attr_based_Policy |
| 9           | An AMI entity with access enters/modifies AMI policy incorrectly, due to a lack of understanding of the policy system. | Secure_Configuration  
User_Auth_Management  
Enrollment_Process |
| 10          | An AMI entity with access enters/modifies AMI policy incorrectly, due to a lack of understanding of the current policy. | I&A |
| 11          | An AMI entity with access enters/modifies AMI policy maliciously to cause information disclosure or loss. | |
| 12          | An AMI entity with access enters inconsistent AMI policy. | |
| 13          | An AMI entity with access imports a malicious AMI organizational policy. | |
Threat Name | Description | Best Practices [Ref Table4.1 and Table4.2]
--- | --- | ---
14 Required organizational policies are inconsistent resulting in denial of service.

Table 4.3: Admin Threats: Best Practices

### 4.5.2 Audit Threats

Audit threats are those threats that involve the AMI audit logs.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entity creates a large number of auditable events in order to cause the AMI audit logs to run out of resource space.</td>
<td>Audit_Log_Maintenance Import_Export_Control Maintain_Online</td>
</tr>
<tr>
<td>2</td>
<td>An AMI entity with proper access to the audit logs fails to clear enough space for the logs, causing the AMI audit logs to run out of resource space.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>An entity causes the AMI auditing function to fail, allowing an entity to perform non-recorded auditable actions.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>An entity reads AMI audit logs when it does not have authorization to read any audit logs.</td>
<td>Audit Confidentiality</td>
</tr>
<tr>
<td>5</td>
<td>An entity reads AMI audit logs with a security attribute it does not possess.</td>
<td>Import_Export_Control</td>
</tr>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table-4.1 and Table-4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>An entity modifies AMI audit logs to hide other actions.</td>
<td>I&amp;A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintain_Online</td>
</tr>
<tr>
<td>7</td>
<td>An entity deletes AMI audit logs it does not have authorization to delete.</td>
<td>Attr_based_Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Admin_Guidance</td>
</tr>
<tr>
<td>8</td>
<td>An AMI entity with proper access misinterprets audit data, and thus cannot</td>
<td>Audit</td>
</tr>
<tr>
<td></td>
<td>detect inappropriate actions of other principals.</td>
<td>Import_Export_Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintain_Online</td>
</tr>
<tr>
<td>9</td>
<td>An AMI entity with proper access cannot find the desired audit data within</td>
<td>Admin_Guidance</td>
</tr>
<tr>
<td></td>
<td>the AMI audit logs, and thus cannot detect inappropriate actions of other</td>
<td>Audit</td>
</tr>
<tr>
<td></td>
<td>principals.</td>
<td>Import_Export_Control</td>
</tr>
<tr>
<td>10</td>
<td>An AMI entity with proper access is not provided enough information by the</td>
<td>Maintain_Online</td>
</tr>
<tr>
<td></td>
<td>AMI audit logs to detect inappropriate actions of other principals.</td>
<td>Admin_Guidance</td>
</tr>
<tr>
<td>11</td>
<td>An AMI entity with proper access is not provided enough information by the</td>
<td>Maintain_Online</td>
</tr>
<tr>
<td></td>
<td>AMI audit logs to identify principals who take inappropriate actions.</td>
<td>Admin_Guidance</td>
</tr>
</tbody>
</table>

Table 4.4: Audit Threats: Best Practices
4.5.3 Download Threats
Download threats are those threats that directly involve the download source interface (patch software, etc).

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An AMI entity with proper access to the Download service asset loads software/configuration into an AMI component resource asset out of sequence.</td>
<td>Import_Export_Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity_Checks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SW_Download</td>
</tr>
<tr>
<td>2</td>
<td>An AMI entity with access to the Download Software service asset loads software/configuration into the wrong AMI component resource asset.</td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import_Export_Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity_Checks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SW_Download</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comp_Attributes</td>
</tr>
</tbody>
</table>

Table 4.5: Downloading Threats: Best Practices

4.5.4 Eavesdropping Threats
Eavesdropping is unauthorized real-time interception of a private communication.

Several Solutions:

- Provide secure session establishment between the system and remote systems using NSA approved confidentiality, integrity, authentication and non-repudiation of network transmissions.
- Restrict user access to cryptographic IT assets in accordance with a specified user access control policy.
- Provide complete separation between plaintext and encrypted data and between data and keys.
- Provide security services and labels on import/export data that is consistent with policy (i.e. user, data source, data content, and intended audience).
- Provide protection of a user or admin session to prevent an unauthorized user from using an unattended computer where a valid user has an active session.
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table 4.1 and Table 4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entity eavesdrops on the Backhaul network in an attempt to read an information asset (e.g., in order to receive covert channel communications or perform traffic analysis).</td>
<td>O.Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>O.Crypto_Comm_Channel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>O.Import_Export_Control</td>
</tr>
<tr>
<td>2</td>
<td>An AMI entity eavesdrops on the AMI Virtual Network in an attempt to read an information asset (e.g., in order to receive covert channel communications or perform traffic analysis).</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>An entity eavesdrops on the Policy Authority Interface in an attempt to read a policy, policy mechanism, or traffic flow information asset.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>An entity eavesdrops on the AMI Systems Interface in an attempt to read information content, information attributes, policy, policy mechanism, or traffic flow information assets.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>An entity eavesdrops on the non-AMI Systems Interface in an attempt to read information content, information attributes, or traffic flow information assets.</td>
<td></td>
</tr>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table4.1 and Table4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>An entity eavesdrops on the Key Management Systems Interface in an attempt to read policy, policy mechanisms, or traffic flow information assets.</td>
<td>Confidentiality Import_Export_Control Session_Protection</td>
</tr>
<tr>
<td>7</td>
<td>An entity eavesdrops on the Users Interface (e.g. via a camera or a tap in the monitor cable) in an attempt to read policy, information content, or information attributes information assets.</td>
<td>Confidentiality Import_Export_Control Session_Protection</td>
</tr>
<tr>
<td>8</td>
<td>A valid AMI user leaves the workstation unattended, does not logout, and leaves the AMI Token in the workstation. An entity sits at the unattended workstation and improperly accesses information assets.</td>
<td>Confidentiality Session_Protection</td>
</tr>
<tr>
<td>9</td>
<td>An entity eavesdrops on the Users Interface because an authorized user viewed information assets in an unauthorized area.</td>
<td>Security_Mgt Comp_Attributes Physical_Security</td>
</tr>
</tbody>
</table>

**Table 4.6: Eavesdropping Threats: Best Practices**

4.5.5 Identification & Authentication Threats
I&A threats are those threats that involve the user identification and authentication process.
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entity discovers user authentication information from an AMI component resource asset.</td>
<td>Confidentiality I&amp;A</td>
</tr>
<tr>
<td>2</td>
<td>An entity discovers user authentication information by external methods (i.e. human intelligence).</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>An AMI entity attempts to crack I&amp;A mechanisms through brute force methods (e.g., a password cracker).</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>An entity is able to guess a passphrase because the passphrase was too simple (e.g., too short, it is “password”, etc.)</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.7: Identification and Authentication Threats: Best Practices

4.5.6 Insider Threats

Insider threats are those threats that directly involve authorized users of the system operating maliciously or negligently. Abnormal insider activity should be detected with high probability, since individual insider threats are negated by discovery. Publicizing the improved detection capability also reduces risk by deterring insider activity. Background checks and audits, authentication, intrusion detection, and software integrity checking are all relevant in this role. Further, it is sensitive to being caught (low goal intensity) so the best defenses against insiders are those that increase the deterrent effect by increased chance of detecting the activity. First, all communication from the head-end to the customer endpoint should be treated as control traffic. As such, authentication of commands should be put in place. Good authentication will prevent man-in-the-middle and spoofing attacks by insiders with access to the AMI communication network. While the head-end systems are clearly not critical cyber assets in the sense of NERC CIP-002 (Cyber security standard by NERC)\(^{56}\), the utility may want to treat them as such and implement personnel and system security management. Measures such as background checks and auditing will deter insiders who attack through physical access to AMI or related systems.

Host-based intrusion detection with software integrity checking of the head-end systems will detect changes to the systems by insiders. Utilities should conduct frequent, irregular audits of head-end output compared against input to ensure that they match. All user commands and actions in the head-end systems should be accountable, which will require logging and strong user authentication.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An AMI entity with access creates, enters, edits, or imports content and labels it with incorrect security attributes resulting in unauthorized disclosure.</td>
<td>Confidentiality Import_Export_Control</td>
</tr>
<tr>
<td>2</td>
<td>An AMI entity with access to an information asset attempts to exfiltrate that information asset to a potential covert channel.</td>
<td>Confidentiality Import_Export_Control</td>
</tr>
<tr>
<td>3</td>
<td>An AMI entity with access to an information asset prints that asset and discloses it to an inappropriate individual.</td>
<td>Confidentiality Import_Export_Control</td>
</tr>
</tbody>
</table>

**Table 4.8: Insider Threats: Best Practices**

4.5.7 Key Management Threats

Key Management threats are those threats that involve the Key Management Systems with which AMI interfaces.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An AMI entity with proper access to the Deliver Keys service asset downloads duplicate keys with different attributes. This can lead to unauthorized access to assets.</td>
<td>Confidentiality Admin_Guidance Crypto_Key_Man</td>
</tr>
</tbody>
</table>

87
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>An AMI entity with proper access to the Deliver Keys service asset downloads weak keys that can be broken. This can lead to unauthorized access to assets.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>An AMI entity with proper access to the Deliver Keys service asset downloads keys with inappropriate attributes. This can lead to unauthorized access to assets.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>An AMI entity with access to the Membership Management service asset fails to report an individual whose keys should be revoked.</td>
<td>Admin_Roles_Access, Confidentiality, Admin_Guidance, User_Auth_Management</td>
</tr>
<tr>
<td>5</td>
<td>Key Management services evolve in ways that are not backwardly compatible with AMI (may be included in KMS).</td>
<td>Crypto_Key_Man</td>
</tr>
</tbody>
</table>

**Table 4.9: Key Management Threats: Best Practices**

### 4.5.8 Malicious code
Malicious code threats are those threats that involve malicious code execution or implantation.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table-4.1 and Table-4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 1           | An entity implants malicious code in an application in order to modify the operating system, other applications, or data leading to disclosure of information assets, modification of information assets, denial of service, repudiation. | Confidentiality
Integrity_Checks
Isolate_Executables
Malicious_Code
Attr_based_Policy |
<p>| 2           | An entity implants malicious code in an application in order to modify the operating system, other applications, or data leading to exfiltration of information assets to potential covert channels.                           |                                                                             |
| 3           | An entity implants malicious code in an application in order to attack external entities through a AMI interface.                                                                                               |                                                                             |
| 4           | An entity implants malicious code in an information asset in order to gain access to an asset it is not authorized to access.                                                                                  |                                                                             |
| 5           | An entity implants malicious code in an information asset in order to exfiltrate information assets to a potential covert channel.                                                                              |                                                                             |
| 6           | An entity implants malicious code in an AMI component information asset in order to modify information assets.                                                                                            |                                                                             |</p>
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
</table>
| 7           | An entity causes a user to execute malicious code in an AMI component information asset in order to modify information assets. | Integrity_Checks  
Isolate_Executables  
Malicious_Code |
| 8           | An entity causes a user to execute malicious code in an information asset in order to gain access to an asset. | Confidentiality  
Integrity_Checks  
Isolate_Executables |
| 9           | An entity causes a user to execute malicious code in an information asset in order to exfiltrate information assets to a potential covert channel. | Malicious_Code |
| 10          | An entity implants malicious code in an AMI component resource asset in order to gain access to an asset. | Confidentiality  
Integrity_Checks  
Isolate_Executables |
| 11          | An entity implants malicious code in an AMI component resource asset in order to exfiltrate information assets to a potential covert channel. | Malicious_Code  
Attr_based_Policy |
<p>| 12          | An entity implants malicious code in an AMI component resource asset in order to modify information assets. |  |</p>
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
</table>
| 13          | An entity causes a user to execute malicious code in an AMI component resource asset in order to gain access to an asset it is not authorized to access. | Integrity_Checks  
Isolate_Executables  
Malicious_Code |
| 14          | An entity causes a user to execute malicious code in an AMI component resource asset in order to exfiltrate information assets to a potential covert channel. |                          |

Table 4.10: Malicious Code Threats: Best Practices

4.5.9 Operational Denial of Service (DOS) Attack

Operational denial of service threats are those threats that affect availability of the system and may be caused by operational users of the system.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
</table>
| 1           | An entity enters access control attributes related to specific content resulting in denying access to consumers who should be authorized for that information object. | Import_Export_Control  
I&A  
Integrity_Checks |
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
</table>
| 2           | An entity enters improper value in the priority attribute related to specific content resulting in reduced distribution efficiency for that information object. | Integ_Data  
NonRepudiation  
Obj_Attr  
Session_Protection  
User_Attributes  
Attr_based_Policy  
User_Guidance |
| 3           | An entity creates excessive volume of information objects resulting in resource exhaustion (e.g., storage space) resulting in a denial of service. | I&A  
NonRepudiation  
Resource_Quotas  
Session_Protection  
User_Attributes  
Attr_based_Policy |
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>An entity removes or changes endorsements on an information object in an unauthorized manner with the intent to stop the publication of the information object.</td>
<td>Import_Export_Control I&amp;A Integrity_Checks Obj_Attr Session_Protection User_Attributes Attr_based_Policy</td>
</tr>
</tbody>
</table>
| 5           | An entity enters (regrades to) incorrect values in the access control attributes that overly restrict access to the information content resulting in denial of service. Incorrect values could be as a result of:  
  - Negligence  
  - Hidden or malicious content  
  - Content different than what was displayed | Import_Export_Control I&A Integrity_Checks Obj_Attr Session_Protection User_Attributes User_Guidance |
<p>| 6           | An entity publishes the information object to an excessive volume of ownership types resulting in resource exhaustion (e.g., storage space). | Attr_based_Policy Resource_Quotas |
| 7           | An entity deletes an object it is not authorized to delete resulting in denial of service. | I&amp;A Integrity_Checks |</p>
<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>An AMI entity deletes an object it is authorized to delete resulting in denial of service.</td>
<td>Obj_Attr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Priority_Of_Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Session_Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User_Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attr_based_Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NonRepudiation</td>
</tr>
</tbody>
</table>

**Table 4.11: Operational Denial of Service Attacks: Best Practices**

### 4.5.10 Operational integrity threats
Operational integrity threats are those threats that affect integrity of the system or information in the system and may be caused by operational users of the system.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entity modifies an information asset it is not authorized to modify.</td>
<td>I&amp;A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity_Checks</td>
</tr>
<tr>
<td>2</td>
<td>An entity modifies information content it is not authorized to modify</td>
<td>Integ_Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Obj_Attr</td>
</tr>
<tr>
<td>3</td>
<td>An entity modifies access control attributes when it does not have regrade function access</td>
<td>Session_Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User_Attributes</td>
</tr>
<tr>
<td>4</td>
<td>An entity modifies information attributes it is not authorized to modify</td>
<td>Attr_based_Policy</td>
</tr>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table-4.1 and Table-4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>An entity modifies policy it is not authorized to modify</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>An AMI entity with access in a remote information system attempts to modify AMI information objects in an unauthorized manner.</td>
<td>I&amp;A, Integrity_Checks, Integ_Data, Obj_Attr, Session_Protection</td>
</tr>
<tr>
<td>7</td>
<td>An entity modifies an AMI component software or operating system resource asset in an unauthorized manner.</td>
<td>I&amp;A, Integrity_Checks, Integ_Data, Obj_Attr, Session_Protection, User_Attributes, Attr_based_Policy</td>
</tr>
</tbody>
</table>

**Table 4.12: Operational Integrity Threats: Best Practices**

### 4.5.11 Operational Non-Repudiation Threats

Operational non-repudiation threats are those threats that affect the ability to perform non-repudiation of information in the system and may be caused by operational users of the system.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table-4.1 and Table-4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>An entity enters, edits unauthorized values in the information attributes resulting in false attribution of the content creator.</td>
<td>Import_Export_Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>I&amp;A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NonRepudiation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Session_Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User_Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attr_based_Policy</td>
</tr>
<tr>
<td>2</td>
<td>An entity enters, edits unauthorized values in the information attributes resulting in false attribution of the information object copier. (X says Y did it)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>An entity improperly enters, edits unauthorized values in the information attributes resulting in false attribution of the content endorser. (X says Y signed it).</td>
<td></td>
</tr>
</tbody>
</table>

**Table 4.13: Operational Non- Repudiation Threats: Best Practices**

### 4.5.12 Social Engineering Threats:
Social engineering threats are those threats that involve human-to-human breaches in security.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entity co-opt an AMI user to grant the entity system access.</td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>I&amp;A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical_Security</td>
</tr>
<tr>
<td>2</td>
<td>An entity persuades a user of a non-AMI system with some level of access to AMI to divulge his AMI credentials.</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table-4.1 and Table-4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>An entity persuades a user of a different AMI system with some level of access to the AMI to divulge his AMI credentials.</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>4</td>
<td>An entity persuades an administrator of a non-AMI system to reveal information about system operational procedures, auditing or known flaws so as to enable the entity to access AMI.</td>
<td>Confidentiality Secure_Configuration Evaluated_System</td>
</tr>
<tr>
<td>5</td>
<td>An AMI entity co-opts an AMI user to grant the entity authorization to an asset.</td>
<td>Confidentiality I&amp;A Physical_Security</td>
</tr>
<tr>
<td>6</td>
<td>An entity co-opts an AMI user to access information assets. The attacking entity may then access the information via the co-opted user (e.g., read over the shoulder of user, have user verbally tell content).</td>
<td>Confidentiality User_Attributes User_Auth_Management Physical_Security</td>
</tr>
<tr>
<td>7</td>
<td>An entity co-opts an AMI user to exfiltrate information assets to a potential covert channel.</td>
<td>Confidentiality User_Auth_Management Secure_Configuration</td>
</tr>
<tr>
<td>8</td>
<td>An entity co-opts an AMI user to modify information assets.</td>
<td>User_Auth_Management</td>
</tr>
<tr>
<td>Threat Name</td>
<td>Description</td>
<td>Best Practices [Ref Table-4.1 and Table-4.2]</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>9</td>
<td>An entity attempts to guess a user passphrase based upon knowledge of the user.</td>
<td>Confidentiality, I&amp;A, User_Auth_Management</td>
</tr>
</tbody>
</table>

**Table 4.14: Social Engineering Threats: Best Practices**

4.5.13 Flawed Implementation Threats:
Flawed implementation threats are those threats that arise due to an incorrect or insecure implementation of AMI. Specific threats are listed below.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Description</th>
<th>Best Practices [Ref Table-4.1 and Table-4.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entity exploits flaws in the AMI component [software, hardware] resource assets to gain improper access to assets.</td>
<td>Confidentiality, SW_Download, Malicious_Code, Evaluated_System</td>
</tr>
<tr>
<td>2</td>
<td>An entity exploits flaws in the AMI component [software, hardware] resource assets to perform a denial of service attack.</td>
<td>Confidentiality, SW_Download, Malicious_Code, Evaluated_System</td>
</tr>
<tr>
<td>3</td>
<td>An entity exploits flaws in the AMI component [software, hardware] resource assets to exfiltrate an information asset.</td>
<td>Confidentiality, SW_Download, Malicious_Code, Evaluated_System</td>
</tr>
</tbody>
</table>

**Table 4.15: Flawed Implementation Threats: Best Practices**
CHAPTER 5: Countermeasures for SCADA Vulnerabilities

SCADA system generally refers to monitoring and controlling of equipments that are responsible for delivering power in Smart Grid. Extended functionality of SCADA includes fault detection, equipment isolation and restoration, load and energy management, automated meter reading, and substation control. The SCADA systems used today by the utilities were developed and deployed many years ago. At that time there was no internet, public or private network. Hence, the only security threat was physical destruction of the systems. However, with the introduction of equipment automation and deregulation, SCADA systems needed to have some kind of interconnected network. The need for the remote connections to these control devices exposed the network to a completely new set of vulnerabilities57.

SCADA system works with the corporate environment though it was originally designed to operate as an individual unit. The core intention of the control system design is efficiency and security. Communication protocols like DNP3 which is used for SCADA are designed in order to facilitate communications between various types of data acquisition and control equipment. The protocol was not designed to be secure from hackers, malwares and other malevolent forces that could easily destroy the control systems and disable any critical infrastructure like SCADA. SCADA Network has lot of concern regarding the Security, Authenticity and Integrity in its design, deployment and operation58.

These above mentioned design, communication and behavioral patterns are reasons for the security weakness of the SCADA system. These vulnerabilities in a SCADA like critical infrastructure make it very susceptive to cyber-attacks. Following are the counter measures which need to be implemented in order to make the SCADA system more secure.

5.1 Countermeasures for Master Terminal Unit and Remote Terminal Unit Security Issues:

SCADA system consists of Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) as some of the major components. The other components include communication equipments and SCADA software59.


MTU will be located at central control facility of the operator. It enables the two way connect and control SCADA’s physical equipments. It generally converts the electrical signals coming from the equipment into some digital value like open/closed switch. By receiving, converting and sending these signals, RTU can measure and control the pressure, flow, voltage and current.

The potential and present vulnerabilities in MTU and RTU are due to the publicly available information, vulnerabilities in policy and procedures and also due to vulnerabilities in platform configuration.

Often, too much information about a utility company corporate network is easily available through routine public queries. In addition, significant information on control systems is publicly available—including design and maintenance documents, technical standards for the interconnection of control systems and RTUs, and standards for communication among control devices. This information can be used to initiate a more focused attack against the network. Inadequate security policy for the SCADA, Lack of security procedure documentations and guidelines and improper security architecture and design adds up to the policy and procedure vulnerabilities.

Earlier SCADA hardware, software, and network protocols were proprietary and not made publicly accessible, making it more difficult for the hackers to attack the system as they did not have knowledge about the system. However with growing competition and drive to perform better and reduce cost has led organizations to make a transition from proprietary systems to standardized technologies such as Microsoft’s windows, UNIX operating systems and common networking protocols used by the internet. As a result, the SCADA’s platform got exposed to various vulnerabilities related to Operating Systems, Password and Access Control.

The security issues in the Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) lie mostly within the platform and policy. The best practices for policy vulnerabilities are already explained in the introduction chapter. The following points further highlight the various ways to overcome these security issues.

5.1.1 Counter Measures for Policy and Procedure Vulnerabilities:

Some of the potential vulnerabilities in the SCADA system as discussed by NIST (National Institute of Standards and Technology) in one of its papers presented on “Guide to Industrial Control Systems Securities” are:

---


• Inadequate security policy for the SCADA
• No specific or documented security procedures were developed from the security policy for the SCADA
• Absent or deficient SCADA equipment implementation guidelines
• Lack of administrative mechanisms for security enforcement
• No formal SCADA security training and awareness program
• Inadequate security architecture and design
• Few or no security audits on the SCADA
• No SCADA specific continuity of operations or disaster recovery plan (DRP) and
• Lack of SCADA specific configuration change management

The Information Security Policy in the introduction chapter explains best practices to overcome the policy related vulnerabilities. Figure 5-1 is used to implement the general security policies and procedure. The structure encompasses all the security features that need to be covered in a security policy which can also be applied to SCADA62.

---

5.1.2 Regular Vulnerability Assessments
All of the SCADA equipment has to be regularly assessed to check and see if there is an abnormal operation taking place. These assessments must be done on a regular basis and should recur. Along with the operational units, the other components of SCADA like the corporate network, data base servers, local desktop computers used for customer management should be assessed so that any unseen security gaps in this system can be overcome and increase protection.

5.1.3 Expert Information Security Architecture Design
There are best practices that can be used to overcome most of the security issues in the network. Also a number of new technologies have been developed to combat vulnerabilities such as malware attacks, unauthorized access to systems which are briefly explained in Description section of the Introduction chapter.

5.1.4 Implement the Security Features Provided by Device and System Vendors
Older SCADA networks did not have many security features to protect the system. The utility companies which own the SCADA networks must ask the vendor to provide security patches to the existing system and also produce newer system with enhanced security features. Also factory default security features should not be used because their intent is to provide excellent usability and provide the minimum amount of security. When the default settings are being changed and are not set to its maximum security limits, a thorough risk assessment must be done before those levels are fixed.

5.1.5 Establish Strong Controls over Any Medium That Is Used as a Backdoor into the SCADA Network
Strong authentication must be implemented to ensure secure communications where backdoors vendor connections exist in SCADA system. Modems, wireless and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites. Sending false packets from the enterprise network can attack SCADA system if the SCADA system does not authenticate the packet. It needs to check if the packet is from a authentic source and only then process the packet. Authentication methods such as challenge response, hashing algorithms and digital signatures can be used.

5.1.6 Implement Internal and External Intrusion Detection Systems and Establish 24-Hour-a-Day Incident Monitoring
When abnormal sequence of events takes place on the SCADA network there must be some way to inform the network administrators about this activity. This can be done by using intrusion detection mechanisms where 24 hours tracing of events on the network is recorded.

---

When a security incident takes place either from internal or external sources then there should be techniques and procedures to immediately overcome them based on the level of damage it can cause. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

5.1.7 Conduct Physical Security Surveys and Assess All Remote Sites Connected to the SCADA Network

Automated systems in the SCADA network are most susceptible to attacks since they are unmanned and unguarded. An inventory of all access points and carrying out physical security checks regularly will help to keep a check on any new security issues. Identify and assess any source of information including remote telephone/computer network/ fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Eliminate any points of failure. Prevent unauthorized access to the websites within the enterprise intranet since they provide access to the SCADA system.

5.1.8 Firewalls and Intrusion Detection System

Threats to SCADA network can come from malicious attackers via the internet and hence it is important to monitor the traffic that flows into it. It is important that firewalls and other Intrusion Detection Systems (IDS) (figure 5.2) be installed at the various ingress points (gateways) of the SCADA network to identify malicious traffic before it is allowed to enter\textsuperscript{64, 65}. This will filter out some of the attacks but not all. Hence more rigorous scheme needs to be implemented to overcome the attacks that still manage to flow through. Viruses and worms could swamp the systems with huge volumes of attack traffic. Just having only firewalls and IDS at entry points may not suffice. This leads to the concept of the electronic perimeter.

\textsuperscript{64} Chee-Wooi Ten, Student Member, IEEE, Iowa State University, Manimaran Govindarasu, Member, IEEE, Iowa State University, and Chen-Ching Liu, Fellow, IEEE, Iowa State University 2007, “Cyber security for Electric Power Control and Automation Systems”. [Online]
Available: \url{http://poweryber.ece.iastate.edu/publications/SMC-conf.pdf}

Available: \url{http://www.isa.org/filestore/Division_TechPapers/GlassCeramics/TP04AUTOW046.pdf}
5.1.9 Electronic Perimeter

Traffic flowing from outside sources reaches the gateway where a firewall restricts malicious packets and allows the rest to flow through. The traffic that flows through might still have some malicious packets which could harm the system. Beyond this gateway there is not much filtering that takes place and hence it is important to define and electronic perimeter (figure 5.3) broader so that it filtering takes place once before data reaches the gateway. This perimeter can be formed by multiple intrusion detection systems installed on a wider area. Huge volumes of traffic can be handled by an extended perimeter as it would be possible to stop the attacks further away from the SCADA network. This provides a number of advantages of providing an overlay network in a more distributed and collaborative fashion. It also provides a barrier that always only legal traffic through.

---

Figure 0.3: Electronic Perimeter Implementation in SCADA System

5.1.10 Domain-Specific IDS

The above-mentioned methods i.e. intrusion detection systems installation and electronic perimeter make a baseline protection to provide normal system behavior. In addition, a perspective on an intrusion can be developed by analyzing emerging characteristics. SCADA data can be analyzed in order to look for such patterns. To identify these patterns it is important to have some basic knowledge which is domain specific and also associated with communication devices to construct an IDS attacks signature database. It would require intense analysis of the interconnected grid in order to identify the attack patterns and study them and then generate signatures. However, once this is achieved, the observed behavior needs to be correlated to detect potential intrusions and filter the attack traffic. Hence IDS with these signatures and the secure electronic perimeter can be made to work in a synchronized manner to combat the security issues posed by malware.

5.1.11 Creating Demilitarized Zones (DMZs)

Demilitarized Zones created using firewalls can protect the SCADA network. Multiple DMZs can be created to separate functionalities and access privileges such as peer to peer connections,

---


the data historian, security servers, configurations servers etc. The figure 5.4 below shows the creation of DMZs.

Figure 0.4: Demilitarized Zones Architecture

All the connections can be routed through firewalls and administrators keep a diagram of the local area network and its connections to protected subnets, DMZs, the corporate network, and the outside. Multiple demilitarized zones help from attacks such as virtual LAN hopping, trust exploitation and bring in a better security posture.

5.1.13 Low Latency and High Integrity Security Solution Using Bump In the Wire Technology for Legacy SCADA Systems

The legacy SCADA systems, deployed without security in mind, are vulnerable to sniffing and tampering issues today. The risk is increasing because security through obscurity is failing to protect the system. Achieving security requires a solution, which can retrofit into the legacy SCADA system.

One such solution is “Yet Another Security Retrofit” (YASIR) which is a bump in the wire (BITW) solution for retrofitting security to time-critical communications in serial-based SCADA

---

systems. The goals are to provide high security, low latency, at comparable cost and using standard and patent free tools.

![Figure 0.5: Model for Bump in the Wire Approach](image)

In the figure 7-5, the function of device denoted as S applied on message M which results in frame F. At the receiving end the function of device denoted as D is applied on the message received F'. BITW solution adds to more modules i.e. transmitter T and receiver R in order to provide data authenticity and discards messages from replay attacks.

In the design of transmitter and receiver in YASIR approach, the transmitter applies the encryption algorithm AES-CTR-128 on the frame F thereby providing confidentiality and integrity for the message. Then a time stamp and a unique sequence number are appended to the message for data authenticity and freshness. This solution also provides low latency by using the AES-CTR algorithm. The transmitter relies on the stream nature of the AES-CTR. As and when each byte of the frame F comes in, it will apply the encryption. There is an internal counter, which keeps a count of every 4 bytes in frame F. Once whole message is received it will use the HMAC on the cipher text and internal counter. An iterative HMAC function is used which reduces the storage requirements and has lesser latency [13].

### 5.2 Countermeasures for Enhancing DNP3 Security:

Distributed Network Protocol (DNP3.0) is used in the communication channel between the master and remote terminal unit. Vulnerabilities in the DNP3 protocol layers can be exploited to cause interruption, interception, modification and fabrication of communication between systems. The attacker can capture the message, analyze the traffic pattern, modify parameters such as length field, function code field, destination address, and sequence number field to cause denial of service. An attack on DNP3 takes place either by exploiting the specifications, vendor implementations or weaknesses in the infrastructure using DNP3. Vendor implementations are exploited by attacking the configurations errors in the system. Infrastructure attacks exploit the loop holes in the policies and platform.

---

5.2.1 Countermeasures

In order to combat the above attacks there must be solutions developed which make it more usable and hence provides reliability of data transmitted as well as protected data. In the following points, various solutions are proposed and also how they used overcome the vulnerabilities in the system.

The Security Enhancement approaches are divided into three categories:

1) Solutions that wrap the DNP3 protocols without making changes to the protocols,
2) Solutions that alter the DNP3 protocols fundamentally, and
3) Enhancements to the DNP3 application.

The solutions that wrap the protocols include SSL/TLS and IPSec, which would provide a quick and low-cost security enhancement. The solutions that would require altering the DNP3 protocols tend to be more time-consuming to implement and expensive but provide better end-to-end security, (more application specific security).

5.2.2 Solutions That Wrap the DNP3 Protocols without Making Changes to the Protocols

5.2.2.1 SSL/TLS Solution

Secure Sockets Layer (SSL) / Transport Layer Security (TLS) solution has been used over the internet to provide secure communication over TCP/IP. It provides mutual authentication between the two end points and also preserves the integrity of the data by using digital signatures and privacy via encryption. They prevent man in middle attacks and replay attacks. Now by wrapping DNP3 with SSL/TLS have some advantages like it provides complete security at the protocol level implementation, it’s a fast, effective and straight forward implementation, and also it is security standard for communication protocols.


72 James H. Graham, Sandip C. Patel, Dept. of Computer Engineering and Computer Science

5.2.2.2 **IPSec (Secure IP) Solution**

Instead of providing security at the TCP level, security can be provided at the IP level using IPSec solution.

Since this is placed at a lower level in the stack, it not only protects the IP traffic but in turn protects the TCP traffic as well (See figure 5-7). TCP solution of SSL/TLS could not protect from denial of service or connection reset attack since it was placed at a layer above TCP. But the IPSec solution prevents entry of arbitrary packets and as well as connection reset because connection is done after it is inside the secured network layer. IPSec provides security for all the traffic since it is placed at the lowest level. This solution has some limitations like it is more sensitive to interference by intermediate devices in the communication path, it is less flexible in terms of security provided since it does not provide application specific security but just encrypts every packet and sends it irrespective of its application.

![Figure 5.6: Protocol Stack (Gray-Background Protocols Are Secured Alternatives)](image)

5.2.3 **Enhancements to DNP3 Applications**

The SSL/TLS solution and IPSec solution lack in providing end to end security. Therefore cryptographic techniques can be used in order to provide this level of security.

DNP3 user group had researched on two cryptographic techniques and tested it on a prototype which is presented here\(^\text{74}\).

1. **Authentication Octets**: This is a digital signature based algorithm. Additional bytes are added to the packets which flow from the master to the remote station called as authentication octets. The purpose of adding these bytes is to authenticate the source. Figure 5.7 gives the schematic of how this algorithm is implemented. Authentication octets that are appended to the message are encrypted using the master’s private key. Since the whole message is not encrypted, processing power is saved. The private public keys distribution is this algorithm is assumed to have been stored locally and hence there is no need for certificate authority. The message is also time stamped to avoid replay attacks. The RTU verifies with the time of reception and does not vary from

---
the time of transmission beyond a specified range. At RTU the authentication objects are
decrypted with the public key and compares them with the hash digest calculated
separately by the remote station. If matched the data is unmodified during transit. The
decryption technique makes sure that the message is from an authentic source. But this
method does not protect from eavesdropping. But in SCADA network the requirement
of having better authentication takes priority to eavesdropping.

![Authentication Using Authentication Octets](image)

**Figure 5.7: Authentication Using Authentication Octets**

Authentication via challenge response: In order to overcome man in the middle attack, master
and remote station use challenge and response cryptography.

In this technique both the devices have a shared key. Device which starts communication
initiates a challenge to authenticate the other device. A challenge consists of a random number
generated at the MTU and sent to the RTU. The RTU uses this random number and encrypts it
with the shared key. The result message is sent to the MTU. The MTU decrypts using the shared
key and checks if the decrypted result is same as the random number it originally generated. If
it matches then RTU authenticated itself to the MTU else MTU terminates the connection. In
order to verify authenticity after connection is established, e.g. during times when it receives a
critical command for shut down or when values are out of typical range then RTU can again
send the challenge to MTU.

---

75 Sandip Patel, Information Science & Systems at Morgan State University, Baltimore, Ganesh D. Bhatt,
Department of Information Science & Systems at Morgan State University, James H. Graham, Electrical and
Computer Engineering at the University of Louisville, July 2009, “Improving the Cyber Security of SCADA
Communication Networks”. [Online]
Available: [http://portal.acm.org/citation.cfm?id=1538788.1538820](http://portal.acm.org/citation.cfm?id=1538788.1538820)
The above two solutions were implemented and tested [14] on a testbed at the University of Louisville; the testbed consisted of one master and 5 remote stations. 4 of the remote stations were connected to RTU through Ethernet while the 5th station was connected wirelessly. Snort intrusion detection sensors analyze the communication to extract relevant information to alert the administrator of unauthorized intrusions. The results showed in the table 5-1. Though authentication octets and challenge response takes comparatively more time they also provide enhance security features.

<table>
<thead>
<tr>
<th>Security Approach</th>
<th>Total communication time (in milliseconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Security</td>
<td>325</td>
</tr>
<tr>
<td>With SSL/TLS</td>
<td>373</td>
</tr>
<tr>
<td>With authentication Octets (software encryption)</td>
<td>2146</td>
</tr>
<tr>
<td>With authentication Octets (Hardware encryption)</td>
<td>764</td>
</tr>
<tr>
<td>Challenge response</td>
<td>446</td>
</tr>
</tbody>
</table>

**Table 5.1: Comparison of Security Approaches**

5.2.4 Distributed Network Protocol Version 3 Security (DNPSec)

DNP user group started working on the Secure DNP3 from 2002. DNP3 protocol provides error detection mechanism and also uses sequence number fields to detect duplication of messages. Authentication, encryption or key management was not proposed in the initial version of the protocol. A new mechanism was added to the features of DNP3 present version of the protocol called DNPSecurity (DNPSec)\(^{76}\). The goals of DNPSec are as follows:

- Provide Authentication and Integrity
- Low overhead.
- Support remote key management.
- Built into DNP at application layer.
- Compatible with all communication links supported by DNP.


• Make use of existing standards. 78

There are two main components of the DNPSec. The first is the DNPSec structure to construct the frame and transfer data in secure mode between the Master and the Slave. The second is the key exchange established during the installation and connection setup between the Master and the Slave. [20]

The figure below shows the new frame format for DNPSec [20].

![Figure 5.8 DNP3 Protocol Structure](image)

The protocol structure has a new header which is 4 bytes long. It contains the destination address, MH flag bit which indicates if the packet is from primary host or from the secondary host, the SK flag bit indicates if its new session key for the destination or it has to decrypt with the old session key and has another 14 bits which are reserved. The sequence number indicates the order of the message. It increments with every packet the master sends and cycles back at $2^{32}-1$. When a new session key needs to be established, the present session must be terminated and a new frame with sequence number 0 and new session key must be sent. DNPSec maintains a session key life time period to keep track of the life span of a particular session key. 79

The original link header and payload is protected by encryption (excluding the CRC). It is composed of 264 bytes field containing, 8 link protocol data unit header bytes, 250 Transport Protocol Data Unit bytes, and 6 padding dummy bytes.


The authentication data field contains the integrity check value (ICV). This value is calculated with the sequence number field, original LH field and payload data fields. The function of this field is to provide integrity services and is done by using message authentication algorithm such as, HMAC-MD5-96 or HMAC-SHA-1-96. The steps for evaluation and comparison must be given in the integrity algorithm specification.

5.2.4.1 DNPSec Secure Authentication
DNPSec Secure Authentication is based on the IEC 62351 standards, and is designed to ensure that DNP outstations are communicating with an authorized master and vice versa.

Secure Authentication addresses the following threats:

- Spoofing (where a person or program masquerades as another)
- Modification (where data is modified in transit)
- Replay (where the same operation is replayed)
- Non-repudiation (identifying individual users, and ensuring only authorized users perform critical functions).

While DNP Secure Authentication is not designed to provide encryption or other security measures, such measures can be added outside the DNP protocol.

5.2.4.2 Basic Principles
DNPSec Secure Authentication adheres to the following principles:

- It uses authentication only, not encryption or other security measures. External measures such as bump in the wire link encryptors may be added independently if required.

It is implemented at the application layer, as DNP must be used over a variety of different physical networks and it permits the possibility of protection against rogue applications

- It can be used in transmission direction, master-to-outstation or outstation-to-master.
- It is based on the common security concept of challenge and response as this places the responsibility for security on the device that requires authentication and it permits some communication to be left unsecured if desired.
- It allows for backwards tolerance, so that a secure device may communicate with a non-secure device.
- It follows the security principle of perfect forward secrecy. If a session key is compromised, this mechanism only puts data from that particular session at risk, and does not permit an attacker to authenticate data in future sessions.
- It allows multiple users of the system to be located at the site of the master, and it provides a method to authenticate each of the users separately.
• It allows outstations to limit access to certain functions, based on the identities of individual users.  

5.2.4.3 Scenarios Where Authentication Is Performed

• **Session Initialization:** When a master station initiates a DNP3 session with an outstation/slave, Secure DNP3 will authenticate both stations to prevent spoofing, replay and other attacks. A unique session key is generated and exchanged using pre-shared keys during this phase.

• **Periodic Authentication:** The master station and non-master/slave station will periodically verify their identity to prevent different attacks. The default interval for a periodic authentication is 20 minutes and the maximum is authentication every hour. A new session key is generated and exchanged while performing this periodic update.

• **Requests with Critical Function Codes:** Critical function codes can be the primary target of the attacker. Some example of the critical function codes are: write (FC 2), cold and warm restarts (FC 13, 14) etc. Authentication mechanism is used before responding to these critical function codes.

• **Vendor Specific:** Vendors can implement authentication requirements for other function codes or let end users to choose function codes that require authentication.

5.2.4.4 Modes or Ways of Authentication

• Challenge Response

• Aggressive mode

**Challenge response:** Critical messages received by a challenger require a challenge, unless aggressive mode is used. The challenge must complete successfully before the original message can be processed. Any application message can be challenged, but generally the outstation will challenge controls and other operations which may alter the outstation’s state.

---

Figure 5.9: Message Sequence in Challenge Response

The challenge response works as follows:

- The responder sends the original critical application message to the challenger.
- The challenger replies with a challenge message containing some random challenge data.
- The responder sends a reply message containing an HMAC calculated on information from the original critical application message and the challenge message.
- If the exchange succeeds, the challenger may then process the original critical application message.

**Aggressive mode:** A responder sending a critical message may optionally anticipate the challenge by using aggressive mode. This reduces bandwidth, but at the same time also reduces security.
The aggressive mode sequence is as follows:

- The responder sends the original critical application message to the challenger in aggressive mode, by including an HMAC value calculated on information from this critical application message and the most recent challenge message.
- If the aggressive mode HMAC is valid, the challenger may then process the original critical application message.

5.2.4.5 Key Management
The key management operations in DNP3Sec are very simple to accommodate the static nature of the SCADA environment. They occur during the configuration of the Primary Master host, the Secondary Master host, and the Slaves to establish the initial connection between them; after the re-initialization of the Key Sequence Number (KSN) to generate and distribute a new key to the hosts; and after the timeout of the usage of the session key. The Master host generates and manages a secure database “M_Keydb” for the shared session keys with the Slaves. The database consists of four fields: the Slave address used as an index key to the database, the shared session key, and the time stamp used to limit the usage of the shared key for a certain pre-defined time period, and the Key Sequence Number. The Master calls “M_GenKey” to generate a unique session key when the old session key expired. “M_PutKey” is the function used to insert the new session key into the database. And the M_PutKSN is the function used to insert the new KSN into the database. The Slave needs to maintain two session keys, one for communicating with the Primary Master host and the other for the Secondary Master host. It manages a secure database “S_Keydb” for the shared session keys with the Master hosts. The database consists of three fields and two records: (0, Primary Master Session Key, Key Sequence Number and 1, Secondary Master Session Key, Key Sequence Number). The simple “S_PutKey” is the function used to update the database with a new session key and the “S_PutKSN is the function used to update the database with a new KSN.  

To start a session, the master generates a new set of random session keys, and downloads them to the outstation. This is performed as follows:

- The master sends a key status request to the outstation.
- The outstation replies with a key status message containing some random challenge data.
- The master generates two new random session keys and sends a key change message. The new session keys are wrapped using a key wrap algorithm and the update key.
- The outstation again replies with a key status message. If the exchange succeeded, the key status will indicate that the session keys are valid.
5.2.5 Comparisons of DNP3 Countermeasures

<table>
<thead>
<tr>
<th>SCADA/DNP3 Security Solutions</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Wrapping DNP3 frame with SSL/TLS | • The IEC Technical Committee has accepted SSL/TLS as part of a security standard for their communication protocol  
• Freely available for all common OS  
• Relatively mature | • Run only on a reliable transport protocol (TCP and not for UDP)  
• High performance cost  
• No non-repudiation services  
• Can’t protect data before it is sent or |
after it arrives its destination

- Implementation of the protocol required understanding of the application, OS, and its specific system calls.
- CA are rather expensive and not really compatible with each other

| Wrapping DNP3 frame with IPSec | Protection against DOS  
|                               | Implemented by Operating Systems, Routers, etc.  
|                               | Transparent to applications (below transport layer)  
|                               | No need to upgrade applications  
|                               | Very complex and hard to implement  
|                               | Higher performance cost  
|                               | All devices shall support TCP and UDP communications on port number 20000  

| DNP3Sec | End-to-End security at the application level to support any communication link  
|         | Protocol is simple eliminating the complexity of the key exchange and management issues  
|         | Implement it once for all communication networks  
|         | Required some modification to the DNP3 Data Link Layer  
|         | Theoretical approach, needs to proof the concept (in going work)  

**Table 5.2: Comparisons of DNP3 Countermeasures**
5.2.6 Conclusion

DNP3 was not designed with security capabilities in mind. There are various techniques that be implemented to avoid the attacks on DNP3 protocol. Wrapping of DNP3 protocol structure in SSL/TLS layer or IPSEC layer will provide protection. However, this approach does not provide secure authentication. Another approach is by carrying out protocol enhancements with authentication octets or via challenge response implementation to provide better authentication. Last approach discussed is the DNPSec framework to bring changes in the protocol packet structure to protect against attacks. The SCADA vendors can build such capabilities by utilizing the DNPSec framework with a minimum time and cost without a major impact on the systems components and the application supporting them. The DNPSec framework enables confidentiality, integrity, and authenticity in the DNP3. Such a framework requires some enhancements in the data structure of the DNP3 Data Link layer, without requiring modification to the Master Station and Substation devices and the applications supporting them. Confidentiality and integrity are achieved by encrypting frames between the Master and the Slaves using a common session key assigned at the setup time of the SCADA components. A new session key is established when the frame sequence number reaches the value $2^{32} – 1$ or when the time period for the use of the session key is expired. On comparing these approaches, DNPSec framework provides good security. Authentication is achieved by applying authentication techniques to assure that the sender of the frame is what it claims to be. Proof of concept by testing or simulation could be a future topic worth investigation.\(^{82}\)

5.3 Countermeasures for Enhancing Modbus Security

The Modbus protocol was developed specifically for SCADA and has become the de facto industrial standard. Many vendors use this protocol and develop systems and produce equipment [23]. The vulnerabilities in Modbus Security Attacks can be classified into Serial Only Attacks, Serial and TCP Attacks and TCP only Attacks.

This section talks about the countermeasures that can be applied on Modbus protocol to provide enhanced security. The common security threats are as follows.

When the master sends a message to the field device, it needs to first authenticate the device from which it obtained the packet and then process the packet. Modbus protocol lacks this ability and hence middle man attacks can easily take place in Modbus. This middle man can bombard the slave units with messages and cause denial of service to the original legal master. The middle man can also carry out replay attacks i.e. capture the packets being sent and reuse them by fabricating it to do some other functions.

The best way to solve this issue is by repairing the Modbus protocol at its source. But this will require architecture modifications which are significant changes. Another way to approach this issue is by introducing smaller security mechanisms to protect against attacks.

5.3.1 Secure Modbus Protocol

A secure Modbus protocol must preserve confidentiality, integrity of the message. In order to satisfy these requirements unauthorized entity must not be allowed to access or modify the contents of the message. Also there should not be a middle man who can emulate the master or can negate a performed action.

In the original protocol, there is protocol data unit which is independent of the communication layer. When the Modbus messages are mapped to the structure of the bus or network it introduces additional fields. In the Modbus TCP protocol frame structure there is MBAP header where target address field in serial message packet is replaced by one-byte Unit Identifier in the MBAP Header. Error checking field is removed and length information is added. The length information is stored so that the receiving field device can identify the message boundaries when messages are broken down into packets. The Modbus packet can have variable sized or fixed size data fields. To identify if the entire message is received, in fixed size packets the information is inherent with the function codes. For function codes with variable data sizes there is a byte count field which transfers this information.

The secure architecture that is covered below is intended to satisfy the following security requirements:

1. Integrity of the data is maintained by using a secure hash algorithm. SHA2 (Secure Hash Algorithm) is used to generate the digest and transmitted along with the packet. The integrity is verified by computing the digest with the same algorithm and comparing it.

2. The above scheme does not prevent a middle man to create an own packet and send it to the field device. To avoid this kind of attack it is important to authenticate the master. Therefore a signature based scheme should be used. In this secure Modbus architecture RSA based signature algorithm is used. The master signs the digest with the private key and the field end device will use the public key to release the digest and check on authenticity. With this algorithm even availability will be fulfilled since only the owner with the specific private key can send the packet.

3. The above two schemes don’t provide replay protection. Reason being the packet can be sniffed and obtained by a middle man. Hence a time stamp scheme is used which will help identify if the packet was snifed or is the original packet. The packet structure incorporating time stamp is shown below in the figure 5-14.

---

The Time Stamp (TS) is applied by the master device creating the packet including Modbus Application Header (MBAP) and appended to the packet and sent to the destination. The destination checks this packet along with a pre-defined and configured time interval. If the packet has reached within a time limit then it will be a valid packet. One way of implementing this is by using the Network Time Protocol (NTP). The NTP provides high precision for time interval by synchronizing the clocks of computer systems over packet switched, variable-latency data networks.

NTP requires additional equipment to be installed which is the NTP time server. This server provides reliable clock for all communicating devices.

Since Modbus is a protocol which was developed for old legacy systems in SCADA, applying the above stated extensions to this protocol requires more computing power at master and slave devices. In order to retrofit with the legacy systems a Modbus secure gateway was implemented which carries out the above procedures to make the packet transmission more secure. Figure 5-14 below presents a schematic diagram of the Modbus Secure Gateway.

This gateway is placed between the Modbus master and provides a multi-homed gateway with a TCP/IP interface connected on the master side and a set of point-to-point TCP or serial links connected to legacy slaves. Operation of the gateway is as follows.
When it receives a packet from the master side which flows to the slave, it carries out the following steps.

1. It discards any unauthenticated packets
2. Extracts the Modbus packet by implementing applying the SHA algorithm and checking it the packet has maintained its integrity.
3. It then forwards the packet to the particular slave destination

When it receives a packet from the slave device flowing towards the master it carries out the following steps

1. It creates the secure Modbus packet from the original Modbus packet
2. It signs the packet digest with its private key.
3. Sends the packet over to the master.

The steps to be followed when sending and verifying a secure Modbus packet is as follows

1. The master creates the packet (C) with function code required to carry out that command execution and the slave address. It also Time Stamps (TS) it. (Mreq)
2. Then it computes the digest, encrypts it with the private key (pKm) and sends the request to the slave or the gateway
   \[ C = [TS|Modbus]|SHA2(TS|Modbus)|pKm \]
3. The gateway or slave verifies the packet by using public key (sKm)
   \[ Mreq = Dec(C, PKm) \]

After verifying the benignity of the packet the slave address is read from the MBAP header and sent to the appropriate address. Same procedure is followed when the flow of packets take place other way round.

The following describes the secure survivable SCADA architecture to combat attacks wherein attacker is able to send a command packet to a slave. A command packet is illicit and a firewall will allow it to flow through. Hence when the packet is sent from an illicit source it will still flow through since it is a command packet. Therefore a solution to combat this is presented below.

1. The master composes the packet (C) normally (Mreq) and then the authenticity and integrity of the packet is maintained by using the RSA and SHA algorithms.
2. This packet is then sent to the filtering unit which validates by decrypting (Dec) the packet using the master’s public key.
   \[ Mreq = Dec(C, PKm) \]
3. The filtering unit analyzes the Modbus packet command and destination. If the combination is unusual and dangerous to the slave unit then it will add it into the dedicated stack of malformed packets.

4. If it is an untouched packet then it will authenticate by encrypting (Enc) the message with its own private key pKf and send it to the slave unit.

\[ \text{MrF} = \text{Enc} \{\text{Mr}, \text{pKf}\} \]

5. The slave (PLC) validates the filtered Modbus request (MrF) by the Filtering Unit’s Public Key (PKf)

\[ \text{Mr} = \text{Dec} \{\text{MrF,PKf}\} \]

6. The slave validates the Modbus request (Mreq) with the Master’s Public Key and executes the command

\[ \text{Mreq} = \text{Dec} \{\text{Mr,PKm}\} \]

But there is another security hole in this architecture. If the attacker takes control over both the filtering unit as well as the master then it can reach the slave unit. To avoid this scenario a concept of K-resilience is adopted. This means a mesh of N filtering units which a stronger operating system is deployed between the slave and master unit. The algorithm works in the following manner, when the packet from the master reaches the filtering units, it is sent to at least P filtering units. P should be greater than K. Each filtering unit verifies the authenticity and sends it to the slave unit. If the slave unit at least obtains K number of packets of the same request then it will process the command. Now the attacker has to corrupt P filtering units to reach the slave. Figure 5-15 below shows in detail the proposed architecture.

![Figure 5.15: High Level Secure Survivable Architecture](image-url)

The proposed architecture will provide security in various areas. Does not allow corrupted packet command execution. Because of the signatures used it will provide data integrity. Prevent replay attacks with time stamps. Prevents a malicious master to send corrupted packets.
because of the filters used and also prevents the risk of the attacker reaching the slave through its K-resilience architecture.

The implementation of the prototype is as discussed below. Because of the physical architecture of SCADA the key exchange can be done manually to each system in a secure manner. There is no need for automatic key exchange. The RSA scheme was used for the signature based algorithm. Hence the signature will be applied on the Modbus packet and then encapsulated in the TCP packet. The basic communication layer between the operating system and the Modbus device is guaranteed by a socket, which manage the keep-alive messages, the TCPNODELAY and the TIME-OUT connections.

Components in the master slave unit should be designed for both functionalities of creating a Modbus packet and interpreting the received packet. The Modbus Stream adapter extracts the Modbus packet in the TCP packet and then authenticates it using RSA and checks its time stamp with the TS analyzer. The Modbus ADU Builder/Reader will check if the packet has a valid command to a valid address. It uses the message stack to store all the incoming messages and validate from the intrusion detection system.
CHAPTER 6: Plug-in Hybrid Electric Vehicles

6.1 Introduction

The electric vehicle first made its appearance about a century ago, but it is only in recent years - months, to be more precise - that it has achieved breakthrough status as, the single-most important technological development having a positive impact on society today.

Climate change, over-dependence on fossil fuels, and the current economic crisis have combined to impact the automobile sector to a degree unforeseen, forcing technological innovation to direct its urgent attention toward the development of electric vehicles as an alternative means of transport, and a substitute for internal combustion engines.

It is certainly true that there exist pressures capable of driving the introduction of the PHEV forward, but technological advances are the factors that underpin and give coherence to its development. There are several progressive improvements being made in technology, materials, and power generation and supply, which will support the deployment and use of electric vehicles in the coming years. They include: advances in battery manufacture and electronics (particularly in terms of power); the development of new communication protocols; ever more efficient and flexible information technologies; the growth of renewable energy sources in the electrical energy generation mix; and the concept of smart grids focused on more efficient electricity distribution. All of these improvements are underscored by a much greater degree of passion and personal involvement by the end-user.

The Smart Grid will utilize Vehicle to Grid (V2G) which is one of the technological advances that will be used in making electric vehicles a viable mainstream option for prospective automobile customers. V2G will be a vital component for both the vehicle’s owners and the energy providers because it will allow both parties to draw power from each other as needed. “Peak load leveling is a concept that allows V2G vehicles to provide power to help balance loads by "valley filling" (charging at night when demand is low) and "peak shaving" (sending power back to the grid when demand is high).”\(^{84}\) V2G allows electric vehicle the capability to charge their fuel cells when energy demand is low while energy enables companies to draw power from the vehicles when there is a shortage of power.

Since most vehicles are parked an average of 95 percent of the time, their batteries could be used to let electricity flow from the car to the power lines and back, with a value to the utilities of up to $4,000 per year per car. Seeing that V2G follows the concept of peak load leveling, power consumers and providers can help each other reduce cost and improve overall effectiveness of power distribution. Even though there has been a significant amount of progress in solutions for the PEV related technological problems, other security issues associated with the technology and the data it will use remain to be dealt with.

6.2 PHEV Charging and its Impact:

6.2.1 Battery Charging

Given that charging could be the action having the greatest impact on the electrical sector, there are various alternatives for affecting this. These include:

1) **Substitution**: This involves a rapid exchange of vehicles and/or batteries, and the subsequent charging of both in an offline mode. It would require sharing of cars (vehicle usage and substitution) and battery charging stations for quick and automated battery exchange.

2) **Direct Charging**: This includes regular charging points situated in car parks, shopping centers and residences, and providing battery recharge while the vehicle is parked. There also need to be fast-charging points that could quickly charge a battery in 10 to 15 minutes.\(^\text{85}\)

Offline charging could be the least invasive method given the current system of fuel distribution. A network of "electricity stations" (as opposed to petrol stations) could provide a dedicated system of energy generation in a given location. As for direct charging, given the itinerant nature of user demand and his or her expected freedom to choose a particular charging method or location, this introduces an element of greater uncertainty, and impact on the electricity grid, requiring a system that better adapts to the lifestyle of the user.

6.2.2 Direct Charging and Its Impact on the Electricity Grid

Direct charging depends on various factors - notably battery characteristics (directly related to vehicle performance) and the range of time spans chosen to carry out the recharge. Associated with these are other variables: charging voltage, mode (DC, single-phase AC, and three-phase AC) and the characteristics of the charging systems employed: technology, components and their location, connectors, insulation, and the power and control electronics. All of these variables will influence the charging times, and will vary according to the power input (more power, less time) as shown in the figure below. Therefore, depending on the kind of recharging, there will be an impact not only on the characteristics of the individual charging points but also on the supporting system.

\(^\text{85}\) [http://www.mthink.com/utilities/phevs-are-roll](http://www.mthink.com/utilities/phevs-are-roll)
Based on the charging power input - and this is, of course, related to the methodology employed - it would be possible to fully recharge an EREV battery in about three hours. A fully charged battery would enable operation solely on electrical power for approximately 40 miles, a distance representing about 80 percent of daily car journeys based on the current averages.

For a scenario like this it would be possible to use a charging method of about 4 kilowatt/220 volts.

In terms of the instantaneous power available, the charging method will have a greater or lesser impact, particularly on the distribution assets, depending on how it is carried out. Figure 2 shows how the power varies according to the charging method and the time of day when it is in use, taking into account the daily energy demand curve. We can, therefore, identify different scenarios from the most favorable (slow charging at off-peak times) to the most unfavorable (fast charging at peak times). With the latter we may find ourselves with distribution assets (eg., transformers) incapable of supporting the heavy load of instant energy consumption.
It is necessary to link electric vehicle charging to the daily energy demand curve and instantaneous power availability in such a way that charging impacts the system as little as possible and maximizes the available energy resources. Ideally, there would be a move toward slow charging during off-peak periods. Furthermore, this kind of charging would not impact users as 90 percent of vehicles are not used between 11 a.m. and 6 p.m. Operating under such conditions would also permit the use of excess wind-generated power during off-peak times, enabling a clean locomotion device such as the PHEV to also use renewable (clean) energy as its primary source.

Smart charging would be capable of deciding when to charge in relation to different variables (for example, price and energy availability), and which energy sources to use (in-home energy storage, local and decoupled energy supply, plug-in to the distribution grid, etc.) Supporting the vehicle-to-grid (V2G) paradigm would enable managing and deciding not only when and how to best charge the vehicle, but also when to store energy in the vehicle battery that can later be returned to the grid for use in a local mode as a distributed energy source.

For all of this to be effective, a power and control electronics system (in both local and global mode), supported by information systems to manage those issues, is required. This will enable the optimal charging process (avoiding peak times, and doing fast charging only when necessary) and an intelligent measuring and tariff system. The latter may be either managed by
utilities through advanced meter management (AMM), or virtually through energy tariffs and physical economic transactions.

6.3 Security Issues and Counter Measures:

6.3.1 Privacy
PHEV will over load the smart grid when they are plugged-in for charging because the PHEVs move for place to place so the power requirements to the locations change. For example, there may be a city like Manhattan where more traffic flows in during peak office hours. If many PHEVs are plugged into the grid located at that point, at a time, it will overload the grid. To solve this problem the position of the PHEVs should be monitored all the time. Due to the constant monitoring of the PHEVs, there is no privacy to one’s individual freedom since his PHEV location is being monitored all the time. If someone breaks into the monitoring system, he can get access to this information.

6.3.2 Secure Payment
A very important element to the smart grid is a payment system which works reliably and secure, and which protects both the end-user as well as the provider. There are good reasons to prefer electronic payment systems rather than sticking to cash payments, such as reduced revenue collection costs and a reduce of losses, enhance customer satisfaction, improved services and operational efficiency as well as more flexible pricing strategies. One type of solution is to use credit cards. However credit card systems do have problems as well. For example, transaction needs to be protected so that an individual’s information is not revealed to third parties. Another approach would be to adopt Integrated Transportation Payment Systems (ITPS. Unfortunately, there are also examples of serious shortcomings of today’s ITPS. Existing systems do not have mechanisms protecting their security and especially the privacy of their users. One problem is that some systems deploy cryptographically weak proprietary primitives. Currently e-cash protocols have been extensively studied. The study shows that it is possible to construct secure off-line payment that protect the anonymity of honest users but is nevertheless able to disclose their identities as soon as they try to cheat the system.86

Potential attackers can be categorized as a small set of individuals, commercial companies, and government institutions. Typically regular individuals will attack the system to acquire private sensitive information in order to track other individuals. Individuals will also attack the system because they are curious or because they see it to be a challenge. On the other hand commercial companies will generate user profiles to increase their revenue. They will usually respect legal restrictions but they will also exploit legal loopholes. And finally government institutions will have extensive power and they might even be able to define the legal environment. Therefore it is important to define a legal framework to account for companies and government institutions, and define technical solutions that account for individual attackers.

86 it_security_for_electric_vehicles.pdf
Privacy is a challenging problem, since it involves cryptographic theory, engineering, policy and sociology. In order to enable a deployment, adequate security and privacy mechanisms must be a requirement. To prevent malicious actions by attackers some form of IT security need to be introduced to systems. Such methods range from cryptographic mechanisms, to secure and privacy-preserving payment systems to a critical infrastructure interpretation of the electric car charging network. This should lead us towards addressing the security problems.

6.3.3 Smart Metering

Electricity has no physical form, it can neither be visible nor has any physical weight, and therefore it is very difficult to accurately measure electricity. Knowing this about electricity, that we can make a claim that there will be an inherent incentive for all parties involved in the production and consumption of electricity to be dishonest when reporting the sale of and purchasing of electricity. The owner of the PEV would want to report less electricity than what was actually delivered to the PEV’s batteries, and the energy provider would want to charge for more energy than what was actually delivered. Even worse than these two would be a third party or middle man, such as a charging station, which would be able to cheat both the energy providers and the owners of the PEV. This can all be done if we are not careful in securing the smart meter from tampering.

In order to provide strong protection to this new technology, three defensive techniques are required, which are based on embedded security technologies.

First, the metering data which records the electric energy delivered should be signed using a digital signature within the charging station. A digital signature assures that the data cannot be manipulated later unless an attacker has access to the private cryptographic signature key. Applicable signature algorithms include DSA, RSA or ECDSA, (as specified by The US Federal Information Processing Standard). These algorithms are computationally demanding, but given that a signature has to be derived only every few seconds, even inexpensive embedded CPUs provide sufficient computational resources.

The second crucial component is that the software or hardware module which computes the digital signature is closely linked to the actual metering device. Otherwise, a potential attack could be that the data from the analog metering IC is manipulated as it is being sent to the digital signature module. Even if both ICs are placed on the same circuit board within the “pump”, attacks are possible by manipulating bus data (Such “modchip” attacks are common against video game consoles as the Xbox). In order to prevent the attack, the metering circuit has to be either in the same IC as the digital signature algorithm, or both modules have to be placed in tamper-resistant housing which detects manipulations. Interestingly, such an approach shows similarities to anti-counterfeiting technologies in which products or spare parts are equipped with electronic tags (e.g., RFID tags) which authenticate the part and are physically connected to the target in a tamper-resistance manner.

The third security component assures that the data is hidden during transmission. Even though not absolutely necessary, in most scenarios it will be highly desirable that the metered data is not only protected with a digital signature against alterations, but also encrypted as it is being
transmitted, e.g., to the charging station display or to the utility company. In order to establish such a confidential communication channel, symmetric algorithms like the Advanced Encryption Standard (AES) can be used. If payment information is to be transmitted too, e.g., credit card numbers, encryption will be a crucial requirement.

Both the digital signature and the symmetric encryption rely on cryptographic keys which must be stored securely within the metering station. There are established methods for achieving secure key storage. One of the more challenging aspects of the system will be the key management. Given the distributed nature of the system, using a public-key infrastructure (PKI) seems like a promising approach. A PKI allows to exchange the public keys needed for digital signatures and to compute the symmetric session keys.

6.3.4 Critical Infrastructure and Physical Security

Critical Infrastructures are defined as “complex highly interdependent systems, networks and assets that provide the services essential for a modern society” [PEV-1]. These critical infrastructures are organized into seventeen sectors, including energy, and transportation, which must be protected against malicious attacks. When the PEV’s become the norm and the combustion engine is a thing of the past. The link between the energy and transportation critical infrastructure will become tightly intertwined. Any malicious attack made against either one of these two critical infrastructures could potentially pose as a threat to the security of these two infrastructures, specifically in the areas of traffic management, and payments for services rendered, specifically pertaining to charging of a PEV. Since the link between these two critical infrastructures is in uncharted territory for both the energy and transportation critical infrastructure sectors, studies will need to be made in order to better understand the impacts of such a close relationship between the two sectors. If a malicious attack were to penetrate the defenses of either the energy or the transportation critical infrastructure, it would be devastation to both critical infrastructures, monetarily and physically. Many businesses will not be able to operate without the ability to charge their vehicles. Traffic management will also become a problem, and can potentially lead to physical harm to individuals. Because of the severity of the problems that can be caused by a malicious attack, the Department of Defense should be an active participant in the security of the energy and transportation sectors of the critical infrastructures.

Physical Security of the equipment is also a very important to the security of PEV’s. If an individual is given the chance to take something without paying for it, most of the time that individual will take the opportunity. In this case we are talking about electricity. The Smart chargers will need to be secure enough so that a potential attacker cannot hack the smart charger for a PEV to provide their PEV with free electricity. There also might be attackers out there that are not only looking for free electricity; instead they want to be able to obtain sensitive information from the smart charging of the current owner or previous owners of the smart charging device. This potential security threat can be solved by using encryption and Trusted Platform Modules (TPM), in order to store the encryption keys on the tamper proof module. Sometimes attackers are not just looking to steal information or energy; sometimes they are looking to cause physical harm to the owner of the PEV. If a battery is overcharged
there is a possibility that the battery will explode and cause physical harm to anyone in the vicinity of the explosion. The solution to such a problem should be multi-faceted. The manufacturers of the battery should include circuitry to not allow over charging of their batteries and the smart meter should make sure that over charging of a battery is not allowed. Another place that an attacker can cause mischief is at a charging station for a PEV’s, by either skewing the amount of energy purchased or by stealing credit card numbers via card skimmers. Particular care has to be taken when dealing with the physical security of the hardware that involves PEVs.

Successful integration of PEVs into the Smart Grid depends on overcoming the security challenges of “Secure Payment and Privacy, Smart Metering, and the Critical Infrastructure and Physical Security.”

### 6.4 Tamper-Resistant

PHEV’s devices which are used for metering the power usage, communicating with the towers and other PHEVs must be electronically intelligent, tamper-proof electronics, and backup power. Why are anti-tampering methods important in the United States? At increasingly high electricity rates, a 4 percent loss is enough to get the utilities’ attention. But, even more important, stolen power is the most common power source for illegal marijuana “grow houses.” The power bill for such houses in urban areas can easily hit $10,000 a month, and stealing power from nearby power lines is a convenient way to get it. This could happen in the PHEV’s billing system also if not tamper-proof anyone who knows little about how this device works can use their knowledge to send false information about the power usage from the PHEV and reduce the bill.\(^\text{87}\)

### 6.5 Communication

The PHEVs use cellular network for communication but there are many vulnerabilities in this network that can be used as a means of getting access into the system or sending wrong information, attacking the system etc. The types of attacks are, middle-man-attack, spoofing, fingering and many more.

### 6.6 Security Issues with Networking:

The new trend in the networking world is Cross Platform/Network Systems (CPS). It is one new method that even the smart grid data transmissions such as the PHEVs would rely on. This system has myriad benefits but along with them, there is some security issues cited as well.

We categorize the security issues based on three types of attacks. Traditional attacks in the Internet (TA), newly identified attacks in CPS (NA) and cross-platform attacks (CPA). The cross platform networking system are used in PHEV communication system because the information from the PHEV must be sent to different systems which rely on different networks such as SCADA for power management, DR for pricing information etc. The Internet 3G cross Network

\(^{87}\) [http://www.edn.com/article/CA6643364.html](http://www.edn.com/article/CA6643364.html)
will be the primary channel through which the PHEV will send its information to other systems. The tables below table 6.1 and table 6.2 contain various attack methods and their countermeasures for cross platform networking systems and 3G Cross networks.

### 6.6.1 Cross Platform/Networking Systems

<table>
<thead>
<tr>
<th>Attack Categories</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Attacks (TA)</td>
<td></td>
</tr>
<tr>
<td>TA1: Eavesdropping;</td>
<td>C1: Authentication and Authorization</td>
</tr>
<tr>
<td>TA2: Hijacking/Man-in-the-middle;</td>
<td>C2: Encryption</td>
</tr>
<tr>
<td>TA3: Masquerading</td>
<td>C3: Integrity protection</td>
</tr>
<tr>
<td>TA4: Tempering with Message Bodies</td>
<td>C4: Firewall</td>
</tr>
<tr>
<td>TA5: Denial of Service</td>
<td></td>
</tr>
<tr>
<td>New Defined Attacks in CPS (NA)</td>
<td></td>
</tr>
<tr>
<td>NA1: Malicious Codec Change (MCC) attack</td>
<td>C-NA1: Countermeasure to MCC attack</td>
</tr>
<tr>
<td>NA2: Malicious-formatted packet flooding (MFPF) attack</td>
<td>C-NA2: Countermeasure to MFPF attack</td>
</tr>
<tr>
<td>NA3: Cross-Platform Denial of Service (CPDoS) attack;</td>
<td>C-NA3: Countermeasure to CPDoS attack</td>
</tr>
<tr>
<td>NA4: Malicious code injection and traverse attack</td>
<td>C-NA4: Wireless station hardening and wireless network monitoring based defense</td>
</tr>
<tr>
<td>Cross-platform Attacks (CPS)</td>
<td></td>
</tr>
<tr>
<td>CPA1: Power Management attack</td>
<td>C-CPA1: Synchronization and encryption based defense</td>
</tr>
<tr>
<td>CPA2: Traffic Analysis Attack</td>
<td>C-CPA2: Hiding explicit and implicit identifiers</td>
</tr>
<tr>
<td>CPA3: Packet modification/deletion/replay attack</td>
<td>C-CPA3: Cryptographic approaches</td>
</tr>
</tbody>
</table>

Table 6.1: Categories of Attacks in CPS
### 6.6.2 Internet 3G Cross Network

<table>
<thead>
<tr>
<th>Cross-protocol (Internet-3G)</th>
<th>Key operation</th>
<th>Attacks</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Layer</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDP $\leftrightarrow$ H.245</td>
<td><strong>Signaling Translantion</strong> - Capability Agreement - Codecs Selection - Codecs Modification</td>
<td>TA1: Eavesdropping</td>
<td>C1: Authentication (HTTP Digest, MD5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA1: Eavesdropping (User Account, Network Topology, etc.)</td>
<td>C2: Encryption (IPS, SSL, TLS, PKI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA2: Hijacking/Man in the Middle (Redirect Call)</td>
<td>C3: Integrity Protection and Sequence Number Check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA3: Masquerading (Fake Registration/ Invitation/ Teardown, etc.)</td>
<td>C4: Firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA4: Tampering with SIP Headers</td>
<td>C-NA3: Countermeasure to NA3</td>
</tr>
<tr>
<td></td>
<td><strong>Cross Platform DoS</strong></td>
<td>TA1: Eavesdropping</td>
<td>C2: Encryption (SSL, TLS, PKI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA4: Tampering with SDP Bodies (Include Capability Set, Destination Address and Port, etc.)</td>
<td>C3: Integrity Protection and Sequence Number Check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A2: Malicious Code Change</td>
<td>C1: Codec Modification Authentication</td>
</tr>
<tr>
<td></td>
<td><strong>Media Transformation</strong> - Packet Re-Ordering - Data Extraction - Data Partition - Packet Formation</td>
<td>TA1: Eavesdropping</td>
<td>C-NA3: Countermeasure to NA3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA5: Media packets flooding (DoS, waste resource of transformation module of cross-platform gateway)</td>
<td>C2: Encryption (SRTCP) [21]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A3: CPDoS</td>
<td>C3: Packets Content, Timestamp and Sequence Check</td>
</tr>
<tr>
<td></td>
<td><strong>Media Transcoding</strong> - Audio Decode - Audio Encode - Video Spatial transcoding - Video Temporal transcoding</td>
<td>TA1: Eavesdropping</td>
<td>C-NA3: Countermeasure to NA3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA1: Eavesdropping</td>
<td>C-NA3: Countermeasure to NA3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA5: Media packets flooding (DoS, waste resource of transformation module of cross-platform gateway)</td>
<td>C2: Encryption (SRTCP) [21]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A2: Malicious-formatted packet flooding</td>
<td>C3: Packets Content, Timestamp and Sequence Check</td>
</tr>
<tr>
<td><strong>Transport Layer</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/UDP $\leftrightarrow$ SCCP</td>
<td><strong>Connection Control</strong> - Connection oriented Establishment - Connectionless oriented Establishment - Connection Maintenance</td>
<td>TA1: Eavesdropping</td>
<td>C1: Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA5: UDP request/response flooding</td>
<td>C2: Encryption (IPSec, SSL, TLS, PKI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA2: TCP session Hijacking TCP SYN/ACK flooding</td>
<td>C3: Integrity protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA4: Tampering Message (modification/dereffect/replay)</td>
<td>C4: Firewall (TCP Session Control)</td>
</tr>
<tr>
<td><strong>Network Layer</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP $\leftrightarrow$ MTP3</td>
<td><strong>Route Control</strong> - Routing Selection - Traffic Control - Link Management</td>
<td>TA1: Eavesdropping</td>
<td>C1: Authentication (802.1X, AH/ESP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA2: Hijacking/Man in the Middle (ARP spoofing, ICMP redirection, Malicious Routing Node/Signaling Node)</td>
<td>C2: Encryption (IPSec, PKI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA4: Tampering Message (modification/dereffect/replay)</td>
<td>C4: Firewall (IP and Port Restricted)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA5: Ping flooding, ICMP unreachable Storm</td>
<td>C3: Integrity protection and Sequence Number Check</td>
</tr>
<tr>
<td><strong>Link Layer</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.3 $\leftrightarrow$ MTP2</td>
<td><strong>Link Control</strong> - Flow Control - Re-Ordering - Error Control</td>
<td>TA5: DoS (MAC/CAM flooding, DHCP flooding)</td>
<td>C1: L2 Authentication (802.1X)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA2: Hijacking/Man in the Middle</td>
<td>C4: Firewall (DHCP and MAC/CAM Restricted)</td>
</tr>
</tbody>
</table>

Table 6.2: Attacks and Counter Measures on Internet 3G Cross Networks
CHAPTER 7: DER

A conceptual architecture of the smart grid is depicted in the figure below, it advocates a synergy of computing and physical resources, and envisions a trustworthy middleware providing services to grid applications through message passing and transactions. The architecture also accounts for a power system infrastructure operating on multiple spatial and temporal scales, that infrastructure is a key in supporting the growing penetration of distributed energy resources. There will also be thousands of sensors and actuators that will be connected to the grid and to its supporting information network. Energy generation, transmission, and distribution will be controlled by a new generation of cyber-enabled and cyber-secure energy management systems (EMS) with a high fidelity supervisory control and data acquisition (SCADA) front end.

The information network will merge the capabilities of traditional EMS and SCADA with the next generation of substation automation solutions. It will;

1) Enable multi-scale networked sensing and processing,
2) Allow timely information exchange across the grid and

---

88 Pserc_smart_grid_white_paper_march_2009_adobe7.pdf
3) Facilitate the closing of a large number of control loops in real-time. This will ensure the responsiveness of the command and control infrastructure in achieving overall system reliability and performance objectives.

The benefits from the Smart Grid can be categorized by the three primary stakeholder groups:

- Consumers. Consumers can balance their energy consumption with the real time supply of energy. Variable pricing will provide consumer incentives to install their own infrastructure that supports the Smart Grid. Smart grid information infrastructure will support additional services not available today.

- Utilities. Utilities can provide more reliable energy, particularly during challenging emergency conditions, while managing their costs more effectively through efficiency and information.

- Society. Society benefits from more reliable power for governmental services, businesses, and consumers sensitive to power outage. Renewable energy, increased efficiencies, and PHEV support will reduce environmental costs, including carbon footprint.

Smart Grid, particularly with a full-deployment of smart meters and expected market penetrations of advanced Distribution Automation (DA) devices, PCD and DER, adds a massive volume of data that will need to be managed effectively. The data includes asset installation location and other attributes, device configuration, equipment performance, inspection and maintenance history and pending work orders as well as measurements and controls of Smart Grid devices. Effective management of the data throughout the utility enterprise is essential to reducing Smart Grid/AMI deployment costs, sustaining benefits, and perhaps more importantly manage business continuity risks from deploying far-reaching and transformational technologies like Smart Meter and Smart Grid.

To prepare for the inrush of Smart Grid data that would be generated by the integration of DER into the smart grid, even at the pilot stage, the utility should develop holistic enterprise architecture and integration plans to cover the following, equally important, four areas of need in order of implementation timing:

1) Deployment of Smart Grid systems and devices, including smart meter and in-premise PCD as well as advanced system automation equipment – to ensure efficient installation, and timely and accurate asset data capture during installation.

2) Management of the collected data on Smart Grid asset, system and device configurations – to ensure quality control of the data and that the systems and applications that need the data are updated timely.

3) Operation and maintenance of the Smart Grid assets, including hardware, firmware, and software – to ensure that the system, equipment and devices will be properly maintained from day one.
4) Management and use of data collected from the Smart Grid systems to improve the utility business, including operation efficiency, capital planning and capacity utilization, T&d system and energy efficiency, and customer service.

With all this taken care of, the questions that arise next are: Are the utility’s current cyber security and information protection policies, guidelines, and processes adequate in light of the expanded distributed command and control capabilities as well as the detailed customer usage information data that are becoming available? Do existing system and prospect technology products, and their implementations and integration, provide adequate security measures in their products?

7.1 Physical Security:

Smart Grid will derive its electricity from a combination of renewable and conventional energy sources. Physically, fortifying Smart Grid’s critical infrastructure is a new and daunting challenge because renewable energy facilities in particular spread out over vast distances. Wind is generally viewed as the most likely renewable incremental electricity source over the next several decades. The American Wind Energy Association reports utility-scale turbines for land-based wind installations come with rotor diameters ranging up to 300 feet. DOE indicates typical turbine spacing is five to ten rotor diameters apart, leading to well over a half mile between turbines. DOE concludes generating 20 percent of electricity with land-based wind installations would demand at least 20,000 square miles. By comparison, all US nuclear power plants, which produce roughly 20 percent of power, occupy only 115 square miles.

Smart Grid will require a “backbone” of extra-high-voltage transmission lines, which carry between 345 and 765 kilovolts (kV) of electricity. These power lines will increase the capacity, efficiency, and reliability of the grid. To the extent wind is the source of new generation, tens of thousands of miles of new transmission lines and their support structures will need to be built. Most potential sites for large-scale wind (and solar) farms are removed from population centers. It is estimated that this is going to require literally thousands and thousands of miles of new transmission.

Opinions and Estimates:

A well-marketed wind energy plan, calls for 100,000 wind turbines and 40,000 miles of new high-voltage (>230kV) transmission lines to be built in the Great Plains Region. The physical exposure of this infrastructure could compromise system security, however, as the bulk of new lines will need to be overhead transmission. Experts have suggested burying lines underground will improve Smart Grid’s security. Unfortunately, burying power lines is generally not feasible, as it makes them more susceptible to weather damage and slows repair time. Further, a study by the Edison Electric Institute (EEI) indicated putting power lines underground would cost about $1 million a mile compared with $100,000 to install overhead lines. 89


7.2 Cyber Security

Distributed energy has turned out to be the new trend of the environment conscious authorities and the citizens as well. The outcome of which has come in the form of an urge to integrate Distributed Energy Resources as a means to generate energy for the rising Smart Grid technology. But this integration brings with it a lot of security concerns that could violate the basic working principles and so need to be taken care of as efficiently as possible. Most of the DER security concerns are covered in multiple sections in this document.

If the energy is being generated from a vast generation site at a far of location, the amount of energy being generated and transmitted can be monitored by having a good metering and monitoring system. This method of energy generation is well taken care of as there are authorized personnel involved in these kinds of transmissions.

But with the dawn of technology, citizens are also getting environment conscious and building solar panels on roof tops, backyards, vacant land by their property and any open space available. By doing so they are generating some amount of energy themselves, this energy needs to be accounted for. The advent of smart grid brings along with it features of bi-directional communication between the customer and the vendor, a means by which the customer can send any extra energy being generated to a distribution point so that it could be directed as supply to another line. This sure is a very advanced and well thought of aspect but it brings with it a lot of security issues as well. The AMI is a device that ultimately monitors the amount of energy being consumed or even generated, it keeps track of the entire household consumption and generation information as such. But the drawbacks arise due to it being easily accessible as it is placed at home, within the customers' reach. Due to this many security issues can arise, some of them are listed below;

Cheating Customer: The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use. They would use information freely available from the AMI meter vendor or a standard associated with AMI meters to reset the meter and reprogram it to report false information. If the information is not freely available, the attacker would reverse-engineer a meter to develop a way to modify it. This is very similar to the many cable modem attacks that are openly available. Either the configuration settings from the utility or the actual firmware controlling the operation of the meter would be modified in this attack.

Repudiation: People may generate energy from their personal solar panels, but would not want to give the right information, in which case, they may resort to modifying the AMI data and thus refuse to acknowledge an action that took place. People may physically intrude into AMI system components like Smart Meter to perform unauthorized actions. This is one big threat involved in a person having the freedom to generate energy using DERs.
Insider Attack: The insider attack would take advantage of access to systems at the opposite end from the customer endpoint. The systems that the insider may be able to access include the AMI head-end, the system from which it gets pricing information and the network infrastructure supporting both of those systems. Which cyber-effect an insider uses would depend upon their access to these systems. One with solar panels at his place or other DERs may use the system which generates the pricing information and try to tamper with it.

Unauthorized Access from Customer Endpoint: There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint. The adversary can suborn the customer endpoint, crack wireless communications between the AMI meter and other endpoint equipment, or crack wireless communications from the AMI meter to the local concentrator. These attacks will expose the head end equipment and systems to which the head end is connected. Certain configurations would allow an attacker to affect the bulk electric grid.

PHEV charge points: Such issues would also rise regarding the usage and charging of PHEVs. Customers who own the PHEVs would charge it at their own expense and if they have distributed energy sources, would also provide a charging point to other customers. But how would they keep track of a right billing and payment technique is another area of concern.

Thus we see how the generation of energy using distributed energy resources though does not directly pose a threat but it sure reflects on all its interrelated components, posing vulnerabilities in what should have been a secure grid technique. The freedom and ease of energy generation through distributed energy sources such as wind power, solar power, fuel cells etc. and the feature of bi-directional flow of energy in the new smart grid technology need to be given thought about to avoid the threats mentioned in the table below:

<table>
<thead>
<tr>
<th>Modification</th>
<th>Unauthorized modification of the AMI data. f) Intercept/ Alter g) Repudiation</th>
<th>Integrity</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactions</td>
<td>Interactions of AMI components with the environment could lead to unauthorized access to AMI communication information, modification of AMI data, denial of service to authorized users, and non-repudiation. h) Masquerade i) Bypassing</td>
<td>Confidentiality Integrity Availability Accountability</td>
<td>High</td>
</tr>
<tr>
<td>Controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>j) Authorization Violation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k) Physical Intrusion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>l) Man-in-the-Middle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m) Integrity Violations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n) Theft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o) Replay</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>After-the-Fact</th>
<th>Denial of action that took place or Claim of the action that did not take place is covered under this category.</th>
</tr>
</thead>
<tbody>
<tr>
<td>p) Stolen/Altered</td>
<td></td>
</tr>
<tr>
<td>q) Repudiation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Insider Attack</th>
<th>The insider attack would take advantage of access to systems at the opposite end of the AMI system from the customer endpoint.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
</tr>
<tr>
<td></td>
<td>Low to High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unauthorized Access from Customer Endpoint</th>
<th>There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cheating Customer</th>
<th>The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
</tr>
<tr>
<td></td>
<td>Low to High</td>
</tr>
</tbody>
</table>

**Table 7.1: Threats and Their Impact**
## GLOSSARY

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ACM</td>
<td>Association for Computing Machinery (ACM)</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AES-CTR</td>
<td>Advanced Encryption Standard – Counter Mode</td>
</tr>
<tr>
<td>AMI</td>
<td>Advanced Metering Infrastructure</td>
</tr>
<tr>
<td>AMM</td>
<td>Advanced Meter Management</td>
</tr>
<tr>
<td>AMR</td>
<td>Automated Meter Reading</td>
</tr>
<tr>
<td>Auto-DR</td>
<td>Automated Demand Response</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CBC-MAC</td>
<td>Cipher Block Chaining Messages Authentication Code</td>
</tr>
<tr>
<td>CCMP</td>
<td>Cipher Block Chaining Message Authentication Code protocol</td>
</tr>
<tr>
<td>CIA</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>CMMS</td>
<td>Computer Maintenance Management System</td>
</tr>
<tr>
<td>CPS</td>
<td>Cross Platform System</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
</tr>
<tr>
<td>CSR</td>
<td>Certificate Signing Request</td>
</tr>
<tr>
<td>DA</td>
<td>Distribution Automation</td>
</tr>
<tr>
<td>DER</td>
<td>Distributed Energy Resources</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zones</td>
</tr>
<tr>
<td>DNP</td>
<td>Distributed Network Protocol</td>
</tr>
<tr>
<td>DoE</td>
<td>US Department of Energy</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DR</td>
<td>Demand-Response</td>
</tr>
<tr>
<td>DRAS</td>
<td>Demand Response Automation Center</td>
</tr>
<tr>
<td>DRRC</td>
<td>Demand Response Research Center</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>DSPF</td>
<td>Distribution System Power Flow</td>
</tr>
<tr>
<td>DSM</td>
<td>Demand Side Management</td>
</tr>
<tr>
<td>DSS</td>
<td>Digital Signature Standard</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic-Curve Cryptography</td>
</tr>
<tr>
<td>ECCDSA</td>
<td>Elliptic-Curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>ECCDH</td>
<td>Elliptic-Curve Diffie-Hellman</td>
</tr>
<tr>
<td>EM</td>
<td>Electro-Magnetic</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>EMCS</td>
<td>Emergency Management Control Center</td>
</tr>
<tr>
<td>EPRI</td>
<td>Electric Power Research Institute</td>
</tr>
<tr>
<td>ESP</td>
<td>Energy Service Portal</td>
</tr>
<tr>
<td>FFD</td>
<td>Fully Functional Device</td>
</tr>
<tr>
<td>FH</td>
<td>Frequency Hopping</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>HAN</td>
<td>Home Area Network</td>
</tr>
<tr>
<td>HG</td>
<td>Home Gateway</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating Ventilation &amp; Air Condition</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Transfer Text Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>ICCP</td>
<td>Inter-Control center Communications Protocol</td>
</tr>
<tr>
<td>IDEA</td>
<td>International Data Encryption Algorithm</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Devices</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineer Task Force</td>
</tr>
<tr>
<td>IOU</td>
<td>Investor Owned Utility</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ISO</td>
<td>Independent System Operator</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITPS</td>
<td>Integrated Transportation Payment Systems</td>
</tr>
<tr>
<td>KMS</td>
<td>Key Management Services</td>
</tr>
<tr>
<td>kW</td>
<td>Kilowatt</td>
</tr>
<tr>
<td>kWh</td>
<td>Kilowatt Hour</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MDM</td>
<td>Meter Data Management</td>
</tr>
<tr>
<td>MDMS</td>
<td>Meter Data Management System</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Code</td>
</tr>
<tr>
<td>MITM</td>
<td>Man-in-the-Middle</td>
</tr>
<tr>
<td>NAN</td>
<td>Neighborhood Area Network</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operating Center</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>OASIS</td>
<td>Organization for the Advancement of Structured Information Standards</td>
</tr>
<tr>
<td>OMAC</td>
<td>One-key Message Authentication Code</td>
</tr>
<tr>
<td>OTP</td>
<td>One-Time-Programmable</td>
</tr>
<tr>
<td>OpenADR</td>
<td>Open Automated Demand Response or Open Auto-DR</td>
</tr>
<tr>
<td>PCT</td>
<td>Programmable Communicating Thermostat</td>
</tr>
<tr>
<td>PEV</td>
<td>Plug In Electric Vehicle</td>
</tr>
<tr>
<td>PG&amp;E</td>
<td>Pacific Gas &amp; Electric</td>
</tr>
<tr>
<td>PHEV</td>
<td>Plug In Hybrid Electric Vehicle</td>
</tr>
<tr>
<td>PIER</td>
<td>Public Interest Energy Research</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RCD</td>
<td>Residual Current Device</td>
</tr>
<tr>
<td>RD&amp;D</td>
<td>Research, Development and Demonstration</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFB</td>
<td>Request for Bids</td>
</tr>
<tr>
<td>RFD</td>
<td>Reduced Functional Devices</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>RG</td>
<td>Residential Gateway</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Samir &amp; Adleman Public Key cryptography</td>
</tr>
<tr>
<td>RTO</td>
<td>Regional Transmission Operators</td>
</tr>
<tr>
<td>RTP</td>
<td>Real Time Pricing</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCE</td>
<td>Southern California Edison</td>
</tr>
<tr>
<td>SDLC</td>
<td>Systems Development Life Cycle</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Function Algorithm</td>
</tr>
<tr>
<td>SHS</td>
<td>Secure Hash</td>
</tr>
<tr>
<td>SG</td>
<td>Smart Grid</td>
</tr>
<tr>
<td>SKKE</td>
<td>Symmetric Key Key Establishment</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>TA</td>
<td>Traditional Attacks</td>
</tr>
<tr>
<td>T&amp;D</td>
<td>Transmission and Distribution</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOU</td>
<td>Time to Use</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>UIS</td>
<td>Utility Information System</td>
</tr>
<tr>
<td>USNAP</td>
<td>Utility Smart Network Access Port</td>
</tr>
</tbody>
</table>
VLSI  Very Large Scale Integration
VPN  Virtual Private Network
V2G  Vehicle to Grid
WLAN Wireless Local Area Network
WNAN Wireless Neighborhood Area Network
WPA  Wi-Fi Protected Access
WWAN Wireless Wide Area Network
Wi-Max Worldwide Interoperability for Microwave Access
WSDL Web Service Description Language
WS-Security Web Services Security
XML Extensible Markup Language
XSD XML Schema Definition
REFERENCES


14. REQUEST TO APPROVE PROPOSED CYBER SECURITY STANDARD – By Charles E. Noble


16. False Data Injection Attacks against State Estimation in Electric Power Grids – By Yao Liu, Peng Ning and Michael K. Reiter

http://www.cse.psu.edu/~szhu/papers/tinymesh.pdf

18. Wikipedia; Advanced Metering Infrastructure;
http://en.wikipedia.org/wiki/Advanced_Metering_Infrastructure

19. Open Smart Grid; Shared Documents;
http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx

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


24. http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2futilisec%2famisec%2fshared%20Documents%2f0.%2f0.%2f0.AMI%2f0.Risk%2f0.Assessment
&FolderCTID=&View=[7B63C81F-617F-4FC1-AFCB-8404B6B6B0A7]


26. http://www.sensorsmag.com/files/sensor/nodes/2008/1526/Figure2.jpg


30. Hyung-Joon Kim, IEEE 802.16/WiMax Security, Stevens Institute of Technology, Hoboken, New Jersey

31. P Kitsos, O Koufopavlou, G Selimis and N Sklavos, Low Power Cryptography, VLSI Design Lab, Electrical and Computer Engineering Department, University of Patras.


33. Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.


64. Chee-Wooi Ten, Student Member, IEEE, Iowa State University, Manimaran Govindarasu, Member, IEEE, Iowa State University, and Chen-Ching Liu, Fellow, IEEE, Iowa State University 2007, “Cyber security for Electric Power Control and Automation Systems”. http://powercyber.ece.iastate.edu/publications/SMC-conf.pdf
72. it_security_for_electric_vehicles.pdf
73. [http://www.edn.com/article/CA6643364.html](http://www.edn.com/article/CA6643364.html)