

Energy Research and Development Division
FINAL PROJECT REPORT

**RESEARCH AND DEVELOPMENT
ISSUES FOR CYBER SECURITY IN
THE SMART GRID**



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



MAY 2014
CEC-500-2014-050

PREPARED BY:

Primary Author(s):

Isaac Ghansah PhD

California State University Sacramento
6000 J Street
Sacramento, CA 95819

Contract Number: 500-08-027

Prepared for:

California Energy Commission

David Chambers
Contract Manager

Fernando Pina
Office Manager
Energy Systems Research Office

Laurie ten Hope
Deputy Director
ENERGY RESEARCH AND DEVELOPMENT DIVISION

Robert P. Oglesby
Executive Director

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

Research and Development Issues for Cyber Security in the Smart Grid 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/ or contact the Energy Commission at 916-327-1551.

ABSTRACT

This report discusses research and development issues for Smart Grid information assurance and security. Previous reports discussed 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.

Research and development is needed in situations where the unique characteristics of the Smart Grid as a critical infrastructure require further research, such as patching and update management.

This report is the third in a series of research projects. The tasks addressed in this project were:

- 1) Identifying the potential issues affecting the confidentiality, integrity, and availability of information flow in the Smart Grid system and grouping the issues with respect to confidentiality, integrity and availability.
- 2) Investigating which information security best practice(s) apply to the Smart Grid and to what extent they can be applied. These best practices were intended to mitigate actions that violate confidentiality, integrity and availability of information flow.
- 3) Exploring possible cyber security research and development issues that should be addressed in the Smart Grid. Some of these could involve wireless sensors, wireless communication systems, monitoring and incident response systems.
- 4) Identifying and recommending which potential research and development efforts should and should not be confidential.
- 5) Identifying 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. Researchers identified a number of areas that needed research, including patch management, cost-effective tamper-resistant meters, cryptographic key management and wireless sensors networks.

Keywords: Public Interest Energy Research, PIER, smart grid, electric grid, cyber security, critical infrastructure, information assurance, research, development

Please use the following citation for this report:

Ghansah, Isaac. (University of California Sacramento). 2010. *Research and Development Issues for Cyber Security in the Smart Grid*. California Energy Commission. Publication number: CEC-500-2014-050.

TABLE OF CONTENTS

PREFACE	i
ABSTRACT	ii
TABLE OF CONTENTS	iii
LIST OF FIGURES	iv
LIST OF TABLES	v
EXECUTIVE SUMMARY	1
Introduction	1
Project Purpose.....	1
Project Results.....	1
Project Benefits	2
CHAPTER 1: Introduction	4
CHAPTER 2: General Research Topics	6
2.1 Cost Effective Tamper-Resistance and Tamper-Evidence	6
2.2 Patches and Updates.....	7
2.3 Information Handling Practices.....	7
2.4 Physical Security	8
2.5 Role-Based Access Control (RBAC).....	9
2.6 Trust Management.....	9
2.6.1 Trust Modeling.....	10
2.6.2 Trust Management System	10
2.6.3 Cross-Domain Security.....	11
CHAPTER 3: Potential Research Topics in Cryptography and Key Management	12
3.1 Public Key Infrastructure (PKI).....	12
3.1.1 Trust Establishment	14
3.1.2 Private Key Protection.....	14
3.1.3 Certificate Revocation List (CRL) Availability.....	15
3.2 Key Management and Public Key Infrastructure (PKI).....	15

3.3	Alternative Ways of Obtaining Public Keys.....	16
3.3.1	Identity Based Encryption (IBE).....	16
3.3.2	Trusted Platform Module (TPM).....	19
3.4	Limitation in Devices and Cryptography.....	21
CHAPTER 4: Specific Domain Topics		22
4.1	Choosing a Standard for Implementing NAN.....	22
4.2	Virtual Environment for Customer Domain Gateway	23
4.3	HAN Devices and HAN Gateways Authentication.....	25
4.4	DR Services Providers and Smart Devices Authentication.....	25
4.5	Authentication and Authorization between Users and Smart Appliances and/or HAN-Based Monitors.....	26
4.6	Authentication and Authorization of Users at Field Substations	26
4.7	Key Management for Meters.....	27
4.8	Key Management for Wireless Sensor Networks.....	28
4.9	Side Channel Attacks.....	29
4.10	Enhancing the Security of Serial Communication.....	29
4.11	Trust Management and Plug-in Hybrid Electric Vehicles	29
CHAPTER 5: Wireless Communication Security.....		32
5.1	Security for Routing Protocols in Wireless Mesh Networks.....	32
5.2	IEEE 802.15.4 Security Issues.....	32
GLOSSARY		34
REFERENCES		36

LIST OF FIGURES

Figure 3-1: Signature Generation and Verification.....	13
Figure 3-2: Operations of Identity Based Encryption	17
Figure 3-3: Use of TPM in the HAN Environment.....	19
Figure 3-4: Internal Components of TPM.....	19
Figure 4-1: Virtual Home Flow Chart	24
Figure 4-2: Basic PHEV Networks	30

LIST OF TABLES

Table 4-1: Summary of Technologies Under Consideration for Neighborhood Area Network... 23

EXECUTIVE SUMMARY

Introduction

Information security can help ensure the reliability and safety of data stored in the sophisticated information technology (IT) systems that comprise the Smart Grid as well as ensuring that the electric grid is resilient and reliable. Most IT security systems can be applied to the Smart Grid, but there are potential problems that are unique to the Smart Grid. Research and development (R&D) is needed in situations where the unique characteristics of the Smart Grid as a critical infrastructure require further research, such as patching and update management.

Project Purpose

The goal of this project was to determine information assurance, security, and privacy issues associated with Smart Grid infrastructure and recommend R&D priorities in those areas. Another goal was to identify best practices in information security that can be applied to the Smart Grid system.

Project Results

This report is the third in a series of research documents covering the following Smart Grid cyber security issues, including:

- Potential threats, vulnerabilities and risks.
- Best practices to mitigate those risks.
- Research issues to be addressed in Smart Grid cyber security.
- Privacy issues in smart grid infrastructure.

Some areas of R&D such as cryptographic key management involved multiple components of the Smart Grid and some other R&D topics applied to specific Smart Grid components such as: 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 control generation, transmission and distribution systems and plug-in electric vehicles.

To achieve these objectives the researchers performed the following tasks:

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

Researchers identified a number of areas that needed research, including patch management, cost-effective tamper-resistant meters, cryptographic key management and wireless sensors networks.

Project Benefits

This project helped to:

1. Increase customer trust in the Smart Grid.
2. Increase regulators' understanding of the security issues in the Smart Grid that need to be addressed by manufacturers and utilities.
3. Increase understanding of the privacy issues in the Smart Grid and how they could be addressed.
4. 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:

Introduction

This document is the third of a series of documents 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 Potential Research and Development (R&D) Topics for Smart Grid Cyber Security.

Vulnerabilities, threats, and risks of Smart Grid were covered in the first report, *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk*.¹ Information security best practices that can be used to overcome some of these security vulnerabilities were suggested in the second report, *Best Practices for Handling Smart Grid Cyber Security*.² The best practices document provided solutions to several threats, but there are still areas where the solutions are not adequate. Therefore we are putting forward this document which discusses a number of potential research and development topics for Smart Grid cyber security.

Basic research delves into scientific principles and applied research which uses basic research to better human lives. R&D can be theoretical, experimental, long-term (5-10 yrs), or short-term (less than 5 yrs). This document does not specify which of the above categories each research problem falls into. In many cases the terms research and development are used interchangeably in this document.

The potential research topics are organized as follows:

1) General topics

The covers general topics which could be applied to different domains of the Smart Grid, this includes trust management, cost-effective tamper-resistance and tamper-evident systems, information handling practices, patches, and firmware updates as well as Role-Base Access Control (RBAC).

2) Potential research topics in Cryptography

This section is intended to cover the potential R&D topics with respect to Cryptography and Key Management, which could be implemented in the Smart Grid, such as Public Key Infrastructure (PKI), key management alternatives such as identity based encryption (IBE), Low power encryption techniques, etc.

1 I. Ghansah, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, October 2009.

2 I. Ghansah, "Best Practices for Handling Smart Grid Cyber Security", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, February 2010.

3) Specific domain topics

These research areas cover Neighborhood Area Networks (NANs), Home Area Networks (HANs), Residential Gateways, Demand Response (DR), Supervisory Control and Data Acquisition (SCADA), Distributed Network Protocols (DNP3), Advanced Metering Infrastructure (AMI) as well as Plug-in Hybrid Electric Vehicles (PHEVs). These topics are grouped together because those domains are related to each other.

4) Wireless communication security topics

These are topics which are related to networking but that are not be grouped into the first three categories.

CHAPTER 2:

General Research Topics

2.1 Cost Effective Tamper-Resistance and Tamper-Evidence

Tamper resistance refers to a process, mechanism or device that protects a system from various kinds of tampering, such as unauthorized accesses, unintended information altering and stealing. Tamper evidence refers to a process, mechanism or device that makes the tampering to protected resources/objects become detected. Tamper resistance must be implemented in such a way that the devices, such as meters and other IEDs, are not easily tampered by either local or remote attacks, and by any physical attacks. For example, the devices might be swapped with a fraudulent one. Also, if the devices are attacked by any means, there must be some kind of evidence to indicate that the device has been manipulated. Thus, tamper evidence is also critical in Smart Grid systems. The security mechanisms, such as using cryptography and Intrusion Detection Systems (IDS) or firewalls can help mitigate the risks of being attacked by an adversary. However, since the Smart Grid is required to utilize many different kinds of devices, some mechanism may help reduce the risk of attacks in some devices; while for others it could be inappropriate. For instance, IDS developed for personal computers can be used to secure the incoming/outgoing traffic from/to a proxy machine; whereas, in some devices, such as the power grid sensors and meters, IDS could be embedded into the devices themselves, which may result in the limitation of the features or abilities of the IDS.

Because many smart grid devices such as meters and sensors are embedded systems, energy usage and resource constraints of those devices could introduce another issue. For example, due to the limitation of memory size, embedded systems may not be able to include large signature libraries so it is possible that malicious software like malware and virus may successfully infiltrate the system without detection. Also, false positives could occur when detecting the actions tampered by either natural incidents or adversaries. Furthermore, tamper-resistant/tamper-evidence mechanisms are required to be cost effective and mass producible, since a large number of devices will be deployed in the Smart Grid. Hence, both tamper resistant and evidence must be designed or architected in such a way that they provide security, scalability, secure software and firmware updates, resistance to false positives as well as cost-effective mechanisms.

The research in this area is to provide scalable and cost-effective techniques to improve tamper-resistant mechanisms and make them difficult and/or more time-consuming for an attacker to break into the systems. Also, it should provide the specific ways to prove that the protected object has been tampered with and/or to indicate who might have tampered with it. More importantly, because no single solution can be applied to the entire smart grid system, the research should provide a specific technique to a specific element of the Smart Grid.

2.2 Patches and Updates

Millions of devices, such as IEDs, Smart Meters, etc. will be eventually deployed in the Smart Grid system. There will be some scenarios where software and firmware need to be updated, such as security fixes or software upgrades. The devices must be able to authenticate that the patch that they are downloading comes from a legitimate source; otherwise, any adversary may make use of malware or malicious software to break into the system. Moreover, the mechanisms for software and firmware upgrades will be different in different parts of the smart grid. For instance software upgrades for personal computers or computer gateways may require user consent before updating. Thus, users by themselves can verify that the patches or updates are coming from the intended source. However, in the case of firmware updates on devices such as IEDs, Meters, PLCs, etc., upgrading them cannot be the same as upgrading software. Since millions of devices are deployed in many places and environments, these upgrades must be autonomously performed. Also, there must be mechanisms to authenticate and ensure that the upgrades that will be set into the devices have not been modified at any time. Furthermore, it is possible that after the update has been installed into devices or computers, unexpected consequences could take place to reduce availability constraints. Thus, the maintenance processes and software testing must be considered in the first place.

The research in this area aims to provide a secure patch and update management processes in order to prevent the system from facing the issues specified above.

2.3 Information Handling Practices

Information is sometimes sent to utilities, third party contractors or other entities. The information, such as customers' energy usage and meter information could be shared among those relevant entities. Contractors 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 a secure manner such that only the 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 amount of time that a utility may retain customers' energy usage information must also be specified. There are privacy issues that have to be considered in this area of research as well.

Privacy within Smart Grid is composed of the four dimensions as follows:³

1) Privacy of personal information

Personal information is the information related to an individual in some specific aspects, such as names, photographs, SSN, etc. The privacy of personal information is sometimes called information/data privacy. It involves the right to control and use of data, of individuals with

3 A. Lee, T. Brewer; The Cyber Security Coordination Task Group, "DRAFT NISTIR 7628 - Smart Grid Cyber Security Strategy and Requirements", September 2009 [online]. Available: <http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf>

respect to when, where, how, to whom, and to what extent the information can be shared with and used by others, as well as to guard when the information is disposed appropriately. This dimension is of the most concerns in the areas of Information Technology.

2) Privacy of the person

This is concerned with the right of individuals to control the integrity of an individual's body. Medical treatments and procedures, such as providing blood and tissue sample, and biometric measurements are some of the examples of this dimension.

3) Privacy of personal behavior

This involves the right of individuals to desire freely on their own decisions regarding their activities, such as political activities, sexual preferences, religious practices, etc. It also involves the right to keep certain personal behaviors from being shared with others.

4) Privacy of personal communications

This is the right of individuals to desire the freedom to communicate with others, using various media, without being recorded, monitored or censored.

The information retained in the smart grid systems should be categorized into those four dimensions and must be considered as it can result in the invasion of privacy, if it is not securely protected. Research is needed to determine what types of information in the Smart Grid could create the privacy risks, and to specify the privacy impacts for those four dimensions.

Research in this area should not only to identify how information in the smart grid systems can be stored and managed, but also to identify and describe privacy concerns and impacts within the Smart Grid. The research on the privacy concerns should include, but not limit the following: ⁴

- Exploring how the existing information in the Smart Grid could lead to privacy risks
- Identifying potential privacy problems and impacts
- Providing policies and practices in order to protect privacy and avoid misuse of personal information used within the Smart Grid

2.4 Physical Security

Physical attacks on the devices, such as meters and IEDs could make an attacker gain a cryptographic key and other secret information embedded in the devices because, the key material could be embedded in the device. This may lead to key handling and storage problems, since if the device is stolen or disposed, the knowledge of the secret information retained in the device might be leaked. One possible solution to this is to separate critical information, such as the crypto key into multiple independent parts, so that there must not be

⁴ M. Enstrom, "(DRAFT) Privacy Chapter Introduction", April 06, 2010 [online]. Available:

<http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628PrivacyIntroApr2010>

any single entity possessing enough information by itself to reconstruct the secret. For example, random numbers could be placed into a device along with an out-of-band communication channel. The out-of-band channel could be an activation code or serial number which the user could only obtain confidentially in order to activate the device. To activate a meter, for instance, the maintenance personnel may obtain the activation code by calling the provider. Moreover, if the device has been stolen or removed from the system after the installation, it needs to be re-activated before it can be re-installed into the system in order to ensure that the stolen device is not successfully used by an attacker. The research is to provide the appropriate mechanisms that can handle the issues specified above.

2.5 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.

The problem is that roles of the participants that will utilize the smart grid systems could be different depending on their responsibilities and activities. For example, auditors should have the ability to read and verify states of the devices including remote attestation, but must not be able to configure the devices. Administrators can add, modify and remove users and their rights in the systems and so on. Not only does access control help manage the access and control the operations performed by the users, but it also helps reduce the impact of failure when some part of the system is compromised since no system can be 100 percent secure. Once an adversary can gain access into some part of the system, he or she will be able to perform only the tasks that are allowed for that hacked account. The principle that makes the latter possible is the Least Privilege principle: a subject or entity in the system must be given the privileges that are necessary for its task, but no more. To describe access rules and policies, this principle must be considered. Thus, identifying what appropriate roles for the participants are and what functions should be performed on different Smart Grid environments by those roles is very crucial.

Research in this area should help specify clearly what types of roles users (eg. Auditors, protection engineers, security officers, etc) partake in the system and what operations should be permitted for the roles specified on various components of the smart grid systems. Additionally support for both hierarchical and non-hierarchical roles, emergency bypass of normal role assignment will be needed in keeping with high priority goal of availability.

2.6 Trust Management

Many kinds of elements, such as utilities, consumers and communication networks either local or long-distance transmission, involve Smart Grid systems. Trust management plays the role of determining how an element becomes trustworthy or reliable to others elements, and also in specifying and enforcing security policies to the system. Since the elements could be people, processes or technologies and could perform different operations, identifying who or what should be trusted and to what level is very crucial in Smart Grid systems. For instance, private

networks should be more trusted than public ones. Moreover, access and identity management should be implemented in such a way that only authorized elements can perform certain functions based on their responsibilities. The main issues in trust management are how authorization and authentication between different entities can be implemented. The area of trust management is very broad and requires further researches since eventually there will be the integration of different domains, such as from meters to demand response control centers or from SCADA systems to AMI systems. R&D issues in this area are specified as follows:

2.6.1 Trust Modeling

Trust Modeling is a process of how to define threat profiles and mechanisms that respond to those profiles.⁵ Since there will be a number of elements involved in the system, it is essential to determine how trust can be established and how the degrees of trust can be assigned to an individual or process. It is important to determine what security issues could take place when different domains communicate with each other, and what the impact level and actions corresponding to those issues would be. The major purpose of the trust model is to provide the framework for enforcing security mechanisms of how to respond to those issues.

The research in this area is to develop and refine trust models that could be used as a representative environment to assess the impacts of the security issues across the domains, such as unauthorized accesses, Denial of Service (DoS) attacks, and misconfigurations, as well as to identify strategies to respond to those issues. Also, a trust model must provide the means to authenticate an entity's identity for specific events or transactions. The result of the research should provide a clear view of how to determine specific threats, vulnerabilities, and risks of the specific domain and also the response to those specific threat profiles.

2.6.2 Trust Management System

A trust management system provides a standard approach to specify application security policies, and credentials⁶. One of the common trust management systems that could be implemented in the smart grid systems in order to specify and enforce security policies and access control is KeyNote. KeyNote is designed to work well with a variety of sizes of applications, including large-scale and Internet-based applications. KeyNote provides a standardized language for specifying security policies, trust relationships and digitally-signed credentials that are used to control accesses and requests across untrusted networks. KeyNote could be useful in the smart grid because the security policies are written in a standard language meaning that across the different applications on different domains, the language for expressing and enforcing security policies still remain the same and it is defined outside the application code which makes it easy to alter the policies whenever needed. This report is

⁵ D. Andert, R. Wakefield, and J. Weise, Professional Service Security; Sun Microsystems Inc., "Trust Modeling for Security Architecture Development", December 2002 [online]. Available: <http://www.sun.com/blueprints/1202/817-0775.pdf>

⁶ M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs - Research, A. Keromytis; U. of Pennsylvania, "The KeyNote Trust-Management System Version 2", September 1999 [online]. Available: <http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt>

intended to provide an overview of KeyNote. The further detail of KeyNote which is publicly released is described in RFC 2704⁷.

The research in this area is to take into account the nature of smart grid systems, which is distributed across different domains, on how security policies and credentials can be specified using KeyNote. The outcome of the research should provide the standard security policies, which can be operated on a distributed basis, using a state-of-art trust management system, such as KeyNote.

2.6.3 Cross-Domain Security⁸

Smart Grid consists of power systems domain, IT domain, and if PEVs become an integral part of the grid, transportation domain. The study and research in what adverse activities could be performed in the cyber domain which affect the power domain are not very clear. The need to determine and detect security concerns and impacts from those concerns, such as intrusions, unauthorized accesses, misconfigurations, and to form a correct and systematic response to those concerns, as well as to ensure security without degrading the systems is important. The R&D in this area is to develop models and technologies in order to enhance the reliability of the power system, while ensuring the security in the cyber domain. Also, once the development and implementation of Smart Grid systems become pervasive, a further research into new security risks will be needed. Thus, further research for new security models and technologies will be eventually required.

Examples of research and development in this area are as follows:

- A Large-scaled and reliable security-event detection model that can be used in a cross-correlated manner and can operate on the smart grid without human interference. The model should be scalable enough to be operated on a distributed basis.
- Intrusion detection/prevention system or other technologies using models/methods specified above are necessary. The system should also provide the appropriate strategies to security events on a real-time or near real-time basis. This will help with incident response and forensic capability

⁷ M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs - Research, A. Keromytis; U. of Pennsylvania, "The KeyNote Trust-Management System Version 2", September 1999 [online]. Available: <http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt>

⁸ I. Ghansah; California State University Sacramento, D. Thanos; GE Digital Energy, P. Pal, and R. Schantz; BBN, C. Gunter, T. Yardley, and Himanshu Khurana; University of Illinois, E. Berozet; Elster, S. Klein; OSECS, R. Jepson; Lockheed Martin, J. Ascough, and R. Henning; Harris Corp. P. Blomgren; SafeNet, G. Emelko; ACLARA Tech, K Garrard; Aunigma Network Security Corp, "R&D Themes for Cyber Security in the Smart Grid", March 25, 2010 [online]. Available: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCITGRandD/RDIdeas-March30_2010.doc

CHAPTER 3: Potential Research Topics in Cryptography and Key Management

3.1 Public Key Infrastructure (PKI)

Asymmetric or public key cryptography can be used to implement security goals, such as confidentiality, integrity and non-repudiation. However, to successfully provide these goals, there is the need to ensure that a given public key is from the alleged source and can be trusted. Since the public key is usually made available to the public, it could be published by an adversary as well as the legitimate user. This trust issue has led to the use of Public Key Infrastructure (PKI) and public key certificates. This section is intended to give an overview of PKI related to the issues specified in section 3.1.1, 3.1.2 and 3.1.3.

PKI is a system that is widely used for the establishment and distribution of digital certificates that bind a user's identity and its public key together in order to ensure that the specific public key belongs to the specific identity. The main purposes of PKI are to manage public keys and enable the uses of public key cryptography and digital certificates through the use of Certificate Authorities (CAs) and Registration Authorities (RAs) in insecure environment, such as Internet. Two major components of PKI are as follows:

- **Certificate Authority (CA)**

A CA is "an authority trusted by one or more users to create and assign public key certificates."⁹ The CA is sometimes called a trusted third party which is responsible for providing various key management services and publishing a public key bound to a given user. This is done by having the CA create a message containing the entity's public key and identity and digitally signing the message with its private key. This message is called a digital certificate. The detail of digital signature is described in the next section. 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.

- **Registration Authority (RA)**

In general, RA is an optional component that is used to perform administrative tasks which CA normally performs. A RA is responsible for verifying an entity's certificate request and determining whether an entity is qualified to have a certificate or not.

Overview of Digital Certificate

Digital certificates simply utilize the concept of a digital signature. Figure 3-1 shows the process of signature generation and verification.

⁹ A. Arsenault; Diversinet, S. Turner; IECA, PKIX Working Group, "Internet X.509 Public Key Infrastructure: Roadmap", July 2002 [online]. Available: <http://tools.ietf.org/html/draft-ietf-pkix-roadmap-09>

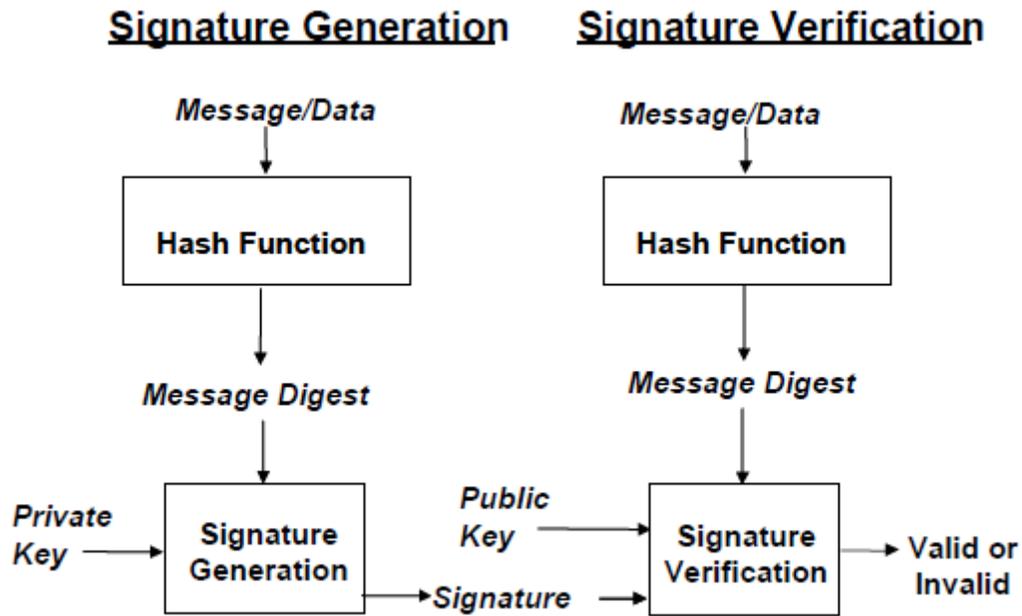


Figure 3-1: Signature Generation and Verification¹⁰

Digital Signature is analogous to a hand-written signature. However, it is very difficult for it to be counterfeited because it can combine the name and identity of the signer. The signature part is generated by using a secure hash function, such as a message digest algorithm, 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 the 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 can provide both source and data integrity.

Typically, a digital certificate contains a public key, certificate information regarding the public key and digital signature of the 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 used to verify if the certificate is valid. The signature part of the certificate is derived from a public key and the credential of the public key owner; it is digitally signed with the CA's private key. The recipient of the certificate uses CA's public key to verify the certificate. Thus, the use of a certificate ensures that the public key in the certificate belongs to the owner or subject of the certificate.

Thus the use of PKI allows for the implementation of digital certificates which are used for ensuring that the public key is certified and comes from the source that it claims. After the public key is considered as the trusted, public key encryption, digital signature techniques, and so on, can be performed.

¹⁰ National Institute of Standard and Technology (NIST), "Digital Signature Standard (FIPS 186-3)", June 2009 [online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

However, implementing PKI is not an easy task. Careful planning and proper design are critical. Thus, there are some research areas, which have to be explored before implementing a PKI, as follows:¹¹

- 1) Trust Establishment
- 2) Private Key Protection
- 3) Certificate Revocation List (CRL) Availability

3.1.1 Trust Establishment

PKI largely relies on trust. To fully utilize PKI, the CA and RA must be trusted and must verify that the identity of the entity requests for a digital certificate is trustworthy. The requesters must be authenticated that they are what they claim to be. The issue is that appropriate and strong verification process must be provided, since CA and RA could be external and internal and could be individually implemented depending on the organization. In addition to the trustworthy verification procedure, the issue of trusting the actual CA needs to be considered as well as the security policy of the CA to ensure that the CA has an appropriate infrastructure and trusted personnel. Even though for years, vendors with infrastructure services have been providing certificate services, there is an issue regarding the cost of the certificates. Also, the ways to utilize certificates from those vendors may not be appropriate when applying those methods to some devices in the smart grid systems since there may be some resource constraints of the devices. Another issue is how to handle in the case where the user's private key has been stolen or lost with or without the notice of the holder of the key and he or she has reported it in order for the certificate to be revoked. A common method in this case is to place the key on a CRL. There are research issues regarding using CRLs for meters which needs to be addressed. There are more details on this in later sections.

3.1.2 Private Key Protection

Compromise of a private key will lead to the breaches in security goals, such as loss of confidentiality, integrity, and non-repudiation, since an adversary can use the private key to decrypt the message or digitally sign the message while pretending to be the actual owner of the key. Not only do the private keys of the users of PKI need to be protected, but the private keys of CAs need to be protected as well. Compromising the CA's private key would allow an attacker to create numerous illegitimate digital certificates and use those certificates for the malicious purposes. Thus, there must be a mechanism to investigate or detect that the private key has been compromised as quickly as possible; otherwise, vast amounts of adverse consequences could take place. To minimize the risk, generally, both the owners of the key, which could be a variety of devices, such as meters and personal computers, or persons, and the authorized issues of the keys must be protected using defensive measures such as Intrusion Detection System (IDS), Antivirus software, etc. Also, secure storage devices must be utilized. Nonetheless, since in the smart grid systems, a wide variety of devices and machines will be utilized, different technologies or means to store the secret information may have to be considered. More importantly, since those devices would operate with nearly no human

¹¹ E.Stavrou, "PKI: Looking at the Risks", January 2005 [online]. Available: <http://www.devshed.com/c/a/Security/PKI-Looking-at-the-Risks/>

interference, there should be the mechanism of how to report to the CA that a device or the key has been tampered with. Thus, there are a number of research issues that should be considered in this area.

3.1.3 Certificate Revocation List (CRL) Availability

Every so often certificates can no longer be considered trustworthy for various reasons including expired certificates, lost or compromised private keys, and the loss of devices that contain certificate information. A CRL is a list containing the serial numbers and revocation dates of all the digital certificates that have been revoked and no longer valid, and maintained by an issuing authority. The CRL is typically available to the public, so that any recipients of a signed message can verify that the certificate received has not been revoked and it is still valid. The issue is that CRL is the only way the CA can invalidate the certificates. Thus, CRL needs to be updated in timely manner. Also, it needs online validation, which may consume bandwidth of the networks. As a result, an adversary may try to attack the availability of the CRL, such as using Denial of Service (DoS) attacks, if the CRL is not available, no operation that depends on the acceptance of the CRL will be carried out. Also, there is the risk that the CRL becomes unavailable due to the machine containing the CRL is infected or compromised, for example; an attacker may be able to use an invalid certificate to trick others for malicious purposes. To minimize the risks associated with the CRL availability, the issuing authority must maintain secure architectures and strong defense mechanisms in order to avoid those security violations and fail-over plans in order to provide secondary architecture whenever the primary one has failed. Thus, there is a need for a research in this area so as to provide solutions to those issues specified above.

3.2 Key Management and Public Key Infrastructure (PKI)

There may be some situations in the Smart Grid where PKI is not appropriate since some devices such as smart meters would not be able to connect to key servers and Certificate Authority (CA). Smart Grid devices may contain both short-term symmetric and long-term asymmetric keys. Also, the smart grid systems will eventually involve millions of devices. Hence, key distribution is one of the potential issues in Smart Grid. The resource limitations of devices also pose some problems with respect to the size of keys and certificates. For example, if the size of certificate is too large, the validation process may be slow and battery life of the device may be shorter than expected. Moreover, the key should be re-negotiated from time to time in order to protect itself and reduce the risk of key being broken. To implement security mechanisms, appropriate key lengths and algorithms should conform to the recommendations from NIST, FIPS, RSA laboratories and other standards. For example, NIST SP800-57 (Part 1)¹² recommends using minimum 2048-bit key for RSA algorithm to protect data beyond 2010. In the case of symmetric algorithms, NIST SP800-57 (Part 1)¹³ recommends using at least three keys

12 E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

13 E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

for triple DES or at least 128-bit key for AES algorithm. However, legacy devices or systems could be used in the Smart Grid systems and may use smaller key size which the designer should include some extra mechanisms, such as time stamping and other techniques, to provide reasonable security level instead of depending on only cryptographic schemes used.

The research in this area is to provide best practices for key management in the Smart Grid, in which key sizes, key lifecycles for each key type and cipher used must be specified. Also, mechanisms to handle the security issues of resource limitations in legacy devices should be specified as well as the methods to deal with key distribution and certificate management in different kinds of environment, where PKI could be applied in the Smart Grid. There are more Key management issues. In cases where symmetric shared keys are used there is a different key management problem from public key systems. The problems are : Will the key be installed in devices at the factory? Will keys be installed by users? What if the keys are changed or need to be changed due to loss, theft, etc.

3.3 Alternative Ways of Obtaining Public Keys

To be able to utilize public key cryptography for encryption and digital signature in a trustworthy manner, certified public keys are needed. This requires that the public key certificates must be available and be obtained prior to using them in order to perform those operations. Also, there are issues of using PKI specified in the section above. There is an interest in the approaches which enable the use of public key cryptography to be performed without satisfying the requirement of retrieving the certified public key in advance. This section gives an overview of two of the possible technologies which are Identity based encryption (IBE) and Trusted Platform Module (TPM). These approaches could be used as an extensions or alternatives to a conventional certificate-based PKI in the Smart Grid as well. Research is needed to determine which of these approaches are appropriate in which areas of the smart grid infrastructure.

3.3.1 Identity Based Encryption (IBE)

Identity-based encryption (IBE) is “a public-key encryption technology that allows a public key to be calculated from an identity and the corresponding private key to be calculated from the public key¹⁴.” IBE enables senders to encrypt messages for the recipient without requiring a recipient’s public key to be established, certified, and published¹⁵. Thus, the complexity of the encryption process for both users and administrators are greatly reduced. The advantage is that the sender does not need to hold the recipient’s public key prior to sending the message, as it can be calculated by the sender. This is different from common public key technologies used in today’s Internet communications which need exchange of keys prior to the start of encrypted communication. The ability to calculate a recipient's public key, in particular, eliminates the

14 G. Appenzeller, L. Martin; Voltage Security, M. Schertler; Tumbleweed Communications, “Identity-based Encryption Architecture”, Internet Draft, November 2007 [online]. Available: <http://tools.ietf.org/html/draft-ietf-smime-ibearch-06>

15 M. Gagné, “Identity-Based Encryption: a Survey”, RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003

need for the sender and receiver in an IBE-based messaging system to interact with each other, either directly or through a proxy such as a directory server, before sending secure messages.

The Figure 3-2 describes the operations of encryption/decryption of an IBE system. The two main components in the IBE are as follows:

- **Private-key Generator (PKG)**

A PKG contains a master secret which is used for generating an individual's IBE private key. An individual needs to send a request for the IBE private key to the PKG and be authenticated before obtaining the IBE private key.

- **Public Parameter Server (PPS)**

A PPS contains IBE public parameters and policy information, such as IBE algorithm and key strength, for an associated PKG. The sender of the message must obtain the IBE public parameter that is used for calculating the recipient's public key from the PPS. The IBE public parameter contains all the information that is necessary for the creation of the encrypted message, except the identity of the recipient. The PPS can also provide the URI (Uniform Resource Identifier) of the PKG where the recipient of an IBE-encrypted message can obtain the IBE private keys. Because the uses of public parameters are very crucial in the IBE, thus the public parameters must be transmitted via a secure communication protocol, such as TLS.

The sender of an IBE-encrypted message chooses the PPS and corresponding PKG according to his security policy. Different PPSs may provide different public parameters, such as different IBE algorithms, different key strengths, or different levels of authentication before granting IBE private keys.

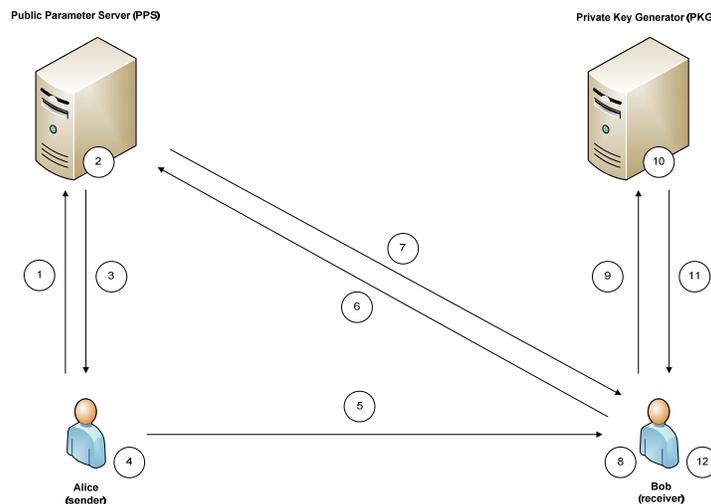


Figure 3-2: Operations of Identity Based Encryption¹⁶

¹⁶ A White Paper by Vertoda, "An Overview of Identity Based Encryption", 2009 [online]. Available: <http://www.slideshare.net/vertoda/an-overview-of-identity-based-encryption>

The steps in figure 3-2 are categorized into the steps of sending IBE encrypted messages and receiving IBE encrypted messages which are described as follows:

Sending IBE encrypted messages

- 1) Alice sends the request for IBE public parameters to the PPS.
- 2) The PPS authenticates the request.
- 3) If step2 is successful, the PPS sends the IBE public parameters to Alice. Then, Alice calculates the Bob's public key by using the public parameters and Bob's identity.
- 4) Alice constructs the encrypted message by choosing a content-encryption key (CEK) and encrypt the data, which she wishes to send to Bob, with that CEK key. Then, Alice uses Bob's public key to encrypt the CEK. Thus, the encrypted message will at least be the combination of the encrypted data and encrypted CEK.
- 5) Alice sends the encrypted message to Bob.

Receiving IBE encrypted messages

- 1) Before Bob can decrypt the message, he needs at least two components, the same public parameters as Alice and the necessary private key. Thus, Bob needs to send the request to the PPS in order to obtain the public parameters that were used in the encryption process.
- 2) If the authentication process is successful, then the PPS sends the IBE public parameters to Bob.
- 3) Bob calculate his own public key by using the public parameters received from the previous step.
- 4) Bob provides the public key, his authentication credentials and the private key request to the PKG.
- 5) The PKG authenticate the request from Bob.
- 6) If step 10 is successful, Bob will obtain the private key from the PKG.
- 7) Bob uses the private key received to decrypt the CEK part of the encrypted message. Then, he uses the CEK to decrypt the encrypted data part of the message.

The concern with IBE is that it requires a centralized server. This means that some keys have to be generated and stored which exposes a threat. The authentication mechanisms used by the PPS and PKG are needed for verifying the requests from both senders and receivers of the messages. Also, it requires secure a channel between a sender or recipient and the IBE servers for transmitting the recipient's private keys and IBE public parameters. Moreover, there may be some issue regarding how the recipient store the private key received from the PKG. Finally, IBE only provides encryption and hence digital signatures must be provided separately. The further details of how to implement IBE can be found in RFC 5408¹⁷.

¹⁷ G. Appenzeller; Stanford University, L. Martin; Voltage Security, M. Schertler; Axway, "Identity-based Encryption Architecture and Supporting Data Structure", January 2009 [online]. Available: <http://tools.ietf.org/search/rfc5408>

3.3.2 Trusted Platform Module (TPM)

Trusted platform module is both the name of published specification detailing a secure crypto-processor that can be used to store cryptographic keys as well as the general name of the implementations of that specification¹⁸. The implementation of TPM is basically a secure micro-controller with cryptographic operations, such as secure the generation of cryptographic keys, hardware pseudo-random number generator, etc.

The Figure 3-3 describes where the TPM could be installed in all the critical end points in the smart grid systems (i.e. Gateway, Smart Meter, Utility head end).

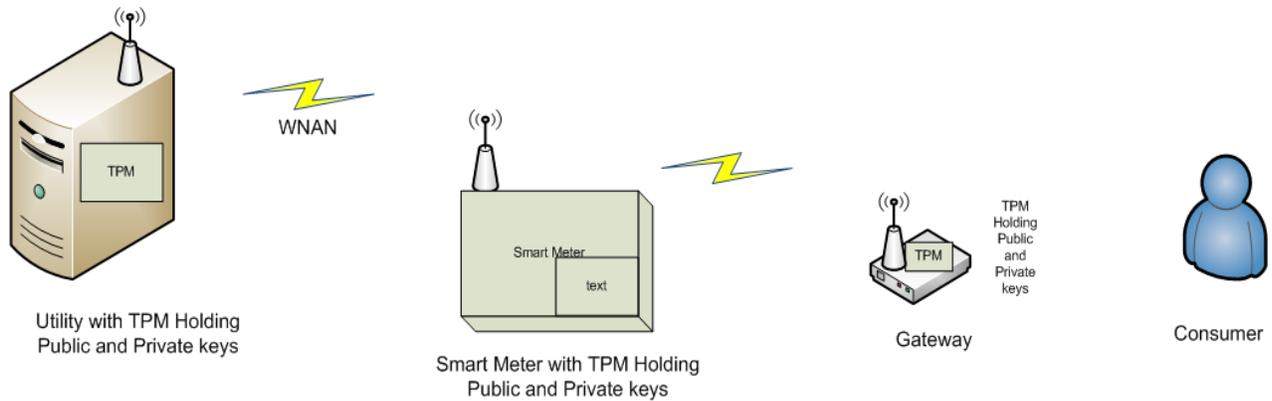


Figure 3-3: Use of TPM in the HAN Environment

In general, putting security services into the hardware and using those in conjunction with software solutions provide higher security level than those that use only software to provide security.

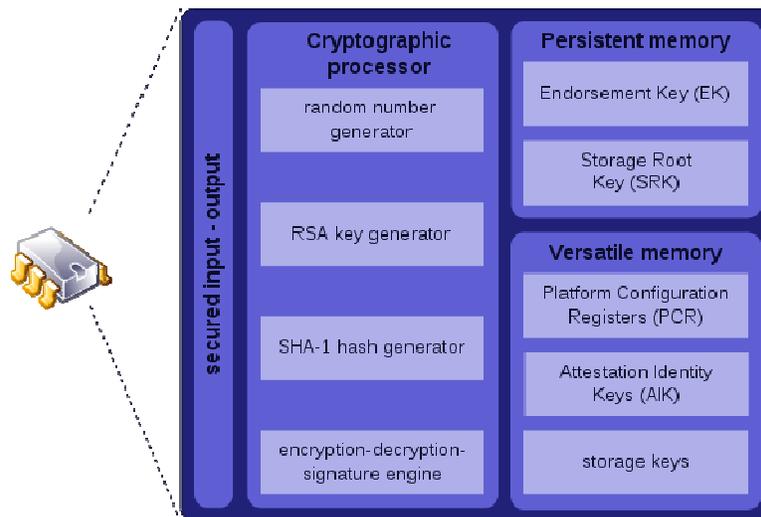


Figure 3-4: Internal Components of TPM¹⁹

¹⁸ Wikipedia, "Trusted Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module

¹⁹ Wikipedia, "Trusted Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module

The TPM provides a set of cryptographic capabilities, such as RSA key generator, random number generator and so on, that allow cryptographic functions to be executed within the TPM hardware²⁰. Hardware and software outside the TPM do not have permission to access and execute these cryptographic functions. TPM contains a hardware engine that is used to perform RSA encryption/decryption by using the Endorsement Key (EK), which is a 2048-bit RSA public/private key pair. The EK is unique and randomly created by the manufacturer and cannot be modified. The private key generated with the TPM never exposes outside the TPM.

Before a TPM machine can be used, the identity of the machine needs to be authenticated with the verifier. Since each TPM has a unique RSA key embedded in the chip at the manufactured time, this key could be used for authentication as well. For example, it can be used to verify that a system that is trying to gain access to is the intended one. However, the use of the EK to authenticate the identity of the TPM may pose privacy concerns to the user, since the EK uniquely identifies the machine. Thus, Attestation Identity Key (AIK) is developed for solving this privacy issues.

The AIK is a key generated for use in attestation. AIK is bound to the TPM's identity, which is in turn tied to the TPM's EK. Whenever, a TPM needs to be authenticated, an AIK will be generated as a second RSA key pair. The public key part of the AIK will be sent to a privacy CA, a trusted third party, to authenticate this public key with respect to the unique EK. If the CA can verify that the EK of that TPM is in its list, it will issue a certificate on that AIK. Thus, the TPM can then use this certificate to authenticate itself with the verifier. Nevertheless, this approach still has the issue that the privacy CA has to be highly available, since, in every transaction, the CA needs to be involved. Also, privacy concerns arise, if the privacy CA and the verifier collude. For example, if somehow the transaction records of the privacy CA are revealed to the verifier, the verifier may be able to uniquely identify the TPM, since the AIK is still tied to the EK.

There is an ongoing research to try to find out the solutions to the issues discussed above. One of the solutions is called, Direct Anonymous Attestation (DAA), which enables remote authentication while preserving the user's privacy. DAA has been included in the latest TPM specification²¹ by Trusted Computing Group (TCG) and is still under development. Thus, there is a need for research in this area on how to deal with the CA availability and privacy concerns in TPM.

The research in this area is to provide the solutions to the issues of the retrieval of the keys and certificates. The two proposed approaches discussed in this section could be one of the solutions. However, given that each of the approaches has their own advantages and disadvantages and since additional techniques would be utilized in order to solve the issues addressed, such as providing digital signature in the IBE or the authentication mechanisms

²⁰ S. Bajikar; Mobile Platform Group, Intel Corporation, "Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper", June 20, 2002 [online]. Available: http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf

²¹ TPM specification, version 1.2, Revision 103. http://www.trustedcomputinggroup.org/resources/tpm_main_specification

used by the PPS and PGK, there is a need for research to address and find the solutions to those issues.

3.4 Limitation in Devices and Cryptography

Smart Grid will be utilizing various kinds of hardware devices, such as sensors, meters, IEDs etc. Those devices may have some resource limitations, such as battery life, bandwidth, CPU and memory. For example, in sensor network, Elliptic-Curve Cryptography (ECC) could be an attractive approach for providing security in Wireless Sensor Networks (WSN), since it utilizes smaller key size and less energy than the cryptographic schemes used in the Internet communications, while providing equivalent security level as other algorithms. However, there is still ongoing research on how much memory a sensor will need in order to keep the secret information, such as keys and certificates, and also how much energy a sensor will consume for the computation of encryption and decryption using different key sizes. Also, resource limitations introduce new kinds of attack which tries to drain battery life and memory resources. Thus, it is necessary to address those limitations and choose the appropriate mechanism in order to ensure security goals as well as overcome those limitations. The outcomes of the research in this area should provide the specific solutions or best practices to those issues addressed above on a specific device.

CHAPTER 4: Specific Domain Topics

4.1 Choosing a Standard for Implementing NAN

There are quite a few technologies in contention to be used to implement neighborhood area network. The technologies under consideration in the implementation of neighborhood area network for Smart Grid are shown in Table 4-1.

Technology	Features	Advantages	Disadvantages
IEEE 802.11 (Wi-Fi)	Data Transfer Rate: 22 Mbps – 128 Mbps* Range: up to ½ mile Operating Frequency: 2.4 GHz to 5 GHz Applications: Meters (AMI), Distribution Automation (DA)	Low device cost Suitable to Mesh topology Low latency	Not yet proven for Smart Grid deployment
IEEE 802.16 (Wi-Max)	Data Transfer Rate: 30Mbps Range: up to 50 km Operating Frequency: 2 GHz to 3 GHz Applications: Meters(AMI), DA, Mobile workforce management	Low latency High bandwidth	High equipment or device cost Not yet proven for Smart Grid deployment
IEEE 802.15.4	Data Transfer Rate: 250 Kbps Range: 100+ meters Operating Frequency: 1 GHz to 2.4 GHz Applications: Meters (AMI), HAN	Suitable for Mesh topology Low power consumption	Lesser data rates Short range coverage
Cellular	Range: up to 50 km Operating Frequency: 900 MHz to 2.4 GHz Applications: Meters (AMI), DA, Mobile workforce management	Uses existing networks Low capital investment Short time-to-market Low module cost	No direct utility control over the network Moderate performance
RF Mesh	Data Transfer Rate: up to 1 Mbps Range: Variable Operating Frequency: variable Applications: Meters (AMI), DA	Customizable based on specific need Self-healing and organizing Low cost	Proprietary Expensive devices Unpredictable Latencies
Leased Lines (e.g. SONET)	Data Transfer Rate: 1.5 Mbps – 155 Mbps Range: Variable Operating Frequency: Wired (Fiber or copper cables) Applications: Substations, DA	High Performance Robust	High recurring cost No direct utility control Not available at all sites

Technology	Features	Advantages	Disadvantages
Broadband over power lines	Data Transfer Rate: 256 Kbps – 10 Mbps Range: Variable Operating Frequency: 1.8 to 80 MHz (electric carrier) Applications: Substations, DA	Low recurring cost Robust	High initial investment Expensive devices Not widely implemented Not reliable
Narrowband over power lines	Data Transfer Rate: 1 Kbps – 100+ Kbps Range: Variable Operating Frequency: 9 KHz to 95 KHz Applications: Meters (AMI), DA	Widely deployed in Europe Proven and Robust	Low performance High latency

Table 4-1: Summary of Technologies Under Consideration for Neighborhood Area Network²²

A preferred standard would be the one which is compatible or common across multiple domains like HAN, NAN and WAN. This would decrease the equipment cost to a great extent and also reduce the complexity of the implementation since the devices would only need to support only one technology standard. If not a single technology, lesser variations used across the domains, the better it is. To explain this in more detail let us consider an example.

The most obvious technology considered for HAN is ZigBee, which is based on IEEE 802.15.4. ZigBee derives the implementation of PHY layer and the MAC layer from the IEEE 802.15.4 standard. If IEEE 802.15.4 is considered for the implementation of NAN, the same radio could be used in the devices installed at homes and utilities. The same packet format could be maintained and so on. This would ease the implementation and lessen the equipment costs.

Also, it would be more advantageous if an existing technology is chosen, or modifying an existing technology to satisfy the Smart Grid NAN deployment requirements. Technologies, such as Narrowband over power lines, which are proven and robust in Europe, could be considered. The advantage of using such a technology is that no new deployments are required as it uses the existing power lines for data transmission, also data could be modulated using the AC 60Hz frequency as a carrier.

To date the researchers know of no proven or widely deployed technology in North America to be used for the implementation of neighborhood area network. Hence research is required in this area to choose a protocol based on the above discussion as well as security issues associated with the protocols.

4.2 Virtual Environment for Customer Domain Gateway

Since a gateway acts like a single point of entry for external entities to enter a home area network, it is being discussed as an ideal platform for virtualization. The virtual environment

²² J. Fox, B. Gohn, C. Wheelock, "Networking and Communications, Energy Management, Grid Automation, and Advanced Metering Infrastructure", PIKERRESEARCH, 4Q 2009.

includes the entire home area and the sensitive data associated with the home area network. One such solution has been proposed by Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu in *A ZigBee-Based Home Automation System*²³. In this they suggest a virtual home which is software constructed in C programming language. The virtual home is implemented on the home gateway. All communication and instructions are checked, as illustrated in Figure 4-1, for security and safety in the virtual environment, before implementation in the real home environment. This is a very effective way to mitigate any intrusion into the real environment. Since this is such a vital contender for providing isolation from the threats, it is also a viable target for attackers, as data which comes from the virtual home is completed is trusted. If this is compromised then attackers can cause serious damage to the home environment. Virtualization can be extended not only to the home area network but can be used in the utility side as well.

There are areas in the virtualization field that need intense research, such as if the network is made scalable how the virtual environment would behave and if the protocols are varied what would be the effect. The entire virtual environment resides in an enclosure which is held in the remote location, which puts constrain on the power requirements. The encryption techniques that are used be low on power budget, whether the virtualization provided will be embedded solution or will it be a completely software based solution. To provide a virtual solution which is power efficient is an area that needs extensive research. The database in the virtual environment is in constant contact during the authentication process is a definitely area of concern, as in what kind of memory will be used to store the sensitive information is an area of research.

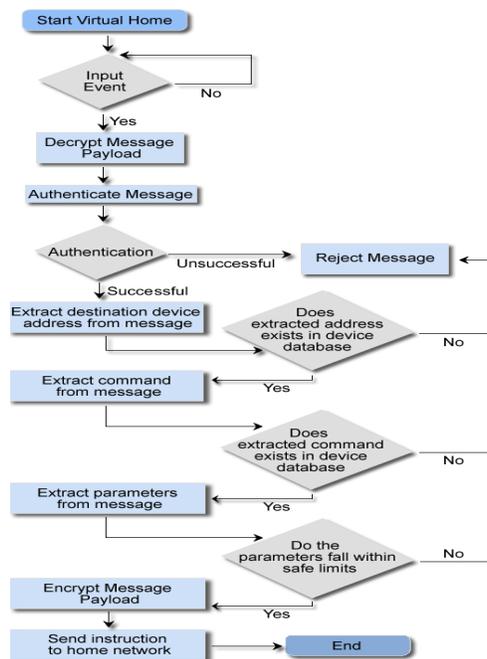


Figure 4-1: Virtual Home Flow Chart

23 K. Gill, S. Hua Yang, F. Yao, and X. Lu; IEEE Transactions on Consumer Electronics, "A ZigBee-Based Home Automation System", Vol. 55, No. 2, May 2009 [online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05174403>

Virtual environment can be a very power and effective tool in the smart grid implementation provided it has been thoroughly researched for loop holes and flawless before deployment.

4.3 HAN Devices and HAN Gateways Authentication

A smart meter and other device could be used as a gateway in order to receive and demand response to DR signals from/to utilities and DR services providers. HAN devices will response to the DR signals received according to DR strategies which could be pre-programmed in the devices. However, it is possible for an attacker to forge a DR command and inject it into HAN. Also, an attacker may be able to join his own device to the network in order to intercept the traffic or perform malicious attacks. It is crucial that authentication mechanisms must be provided in such a way that when a device receives a command, it must be able to ensure that the command is come from the legitimate source and is delivered to the correct device. When the authentication fails, the device should not respond to the signal and/or should be able to report back to the DR head-end. Cryptographic schemes, such as digital signature or message authentication code, could be used to provide such a protection.

Research in this area is needed to provide specific methods for such authentication. However, it is necessary to consider the techniques that can be implemented in different kinds of devices since HAN devices could be gas meters, water meters, lighting controls, in-home monitors, thermostat, etc. Each of the devices may have some limitations, such as resource limitations or inability to store data permanently, and only cryptographic tools may not be sufficient enough to ensure the authentication between those devices. Also, since to some extent, HAN devices could be obtained and installed by consumers, the authentication process should be operated on autonomous basis to simplify things for the consumer.

4.4 DR Services Providers and Smart Devices Authentication

DR signals and control commands could be sent directly from DR Service providers to smart appliances, HAN devices or Energy Management Control System (EMCS) this applies to situations where the signal sent without going through HAN gateways in order to control energy usage by shifting or shedding electrical loads at participant's sites or control the devices. However, an attacker could also send false signals or inject any malicious commands to those devices. If an attacker successfully injects false commands into the system, it could have a tremendous impact on the stability of the grid and energy consumers' billings. Authentication of DR signals sent between DR services providers and other smart appliances is crucial. The system must provide a mechanism to authenticate to ensure that the commands are sent from alleged sources to intended devices properly. If a command is sent in an unauthorized manner the command should be rejected and the devices must not respond to it. Also, the response from the devices should be sent to indicate that the commands received are successfully carried out. Cryptographic techniques, such as digital signature, could provide such a protection. However, devices such as meters, sensors, and other HAN devices, have resource constraints including limited memory, storage, and battery life as well as bandwidth. These limitations should be considered when utilizing mechanisms to provide authentication as well.

The research in this area is to provide specific solutions to those issues addressed above. However, there may be situations where the cryptography may not be utilized adequately, since there will be many different kinds of devices deployed in the smart grid system. The research should also identify these limitations and/or provide best practices or means to handle those issues as well.

4.5 Authentication and Authorization between Users and Smart Appliances and/or HAN-Based Monitors

User authentication is important in smart grid systems, since users could be maintenance personnel, IT personnel or home users. Thus the way to authenticate users should be friendly enough for home users who may not possess technical skills. Password authentication is one of the possible techniques that could be implemented. Currently many smart meters are using this technique to authenticate maintenance personnel. Also, since access to smart devices can be local or remote through AMI or HAN gateway, an attacker may attempt to gain access to the devices as well. Therefore, the system should provide mechanisms to defend the system from password attacks, such as dictionary and brute force attacks, and also limit the attempts to perform those attacks to the system.

Once a user is successfully authenticated and gains access to the system, authorization techniques must be applied. Authorization refers to the act of granting a user or device proper rights to access some particular resource of the system. The issue is that different users could have different functions to perform on the devices. For example, a home user should not have permission to change or reset some important configuration values like energy price and monthly usage in the meter. To provide authorization, access control mechanisms are necessary. Access control mechanisms, such as Role-based Access Control (RBAC), must be described and utilized in order to ensure such that the users can only perform the tasks they are allowed. Details of RBAC are described elsewhere in this report.

Thus, authentication and authorization should be able to ensure that only authorized users can perform certain functions on specific devices.

The research in this area is to describe the potential issues of password attacks that could be manipulated by an adversary and provide defense mechanisms to those issues. Also, it should identify an appropriate set of roles and determine how these roles can perform particular tasks on particular devices. Finally, it should describe access control policies and provide the techniques to implement those policies in the Smart Grid as well.

4.6 Authentication and Authorization of Users at Field Substations

Authentication and authorization of the personnel who work at the substation is an issue that needs research. Authentication and authorization should be provided in such a way that only intended users can be successfully authenticated to assigned devices and can only perform the relevant functions to the users. Authentication and authorization could help reduce the risks of unintended activities and malicious attacks, such as unintended modification of the configuration parameters and unauthorized access. Also, they could help mitigate the risks of

insider attacks by the legitimate personnel, since the users can only perform minimum number of operations which they are allowed to.

The access to the IED's at the substations must be given to a specific user. Generally, it is given to a number of users having specific roles. These systems understand the meaning of the role but are not programmed to allow only the user who is assigned to that role. Therefore, it might be the case that passwords are shared among multiple maintenance personnel; although, the personnel may have different roles. Also, since there are many different devices deployed in a substation, the password that is shared may be common among many systems.

Moreover, the systems can be accessed locally or remotely. Accessing these systems remotely takes place over low speed communication lines. Hence carrying out authentication of the user can slow down the whole communication process. Therefore performing an authentication protocol such as RADIUS or LDAP is undesirable. Finally there should be some methods implemented which will authentication and authorization during emergency situations.

The research is to provide appropriate mechanisms or methods for user authentication and authorization at field substations in the smart grid systems that can tackle those issues specified above.

4.7 Key Management for Meters

Millions of smart meters will be eventually deployed in Smart Grid systems. To ensure security goals, cryptographic keys and other secret information must be contained in those meters in order to provide appropriate protection to AMI networks. Each meter should contain unique key or other secret information that could be used to generate or establish the keys based on the lifecycle of the key and also to protect the meter data from different kinds of attacks, such as eavesdropping, unauthorized modification, etc. Additionally, those keys and secret information contained in the meters need to be re-established and re-distributed at some appropriate point in time. The research on how those keys can be distributed and re-established and what mechanisms should be implemented in AMI systems are necessary. Thus, managing key materials for millions of meters are the potential problems. In some cases a large number of deployed meters may use the same symmetric or shared key across all the meters, perhaps in different states. Proper key management schemes should be implemented in such a way that the knowledge of one key should not result in the compromise of the entire system. Finally, since meters will be deployed across utility and AMI networks, the key management scheme should ensure that compromise of a key in one network will not affect the others.

The research in this area should cover all the aspects of the key management issues, such as cipher suites used and key sizes, key lifecycles, etc., which should be conformed to the NIST SP800-57 (Part 1)²⁴. The research should also provide the solutions to the key distribution and key establishment issues for large scale systems.

²⁴ E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management - Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

4.8 Key Management for Wireless Sensor Networks

Wireless Sensor Networks are expected to be widely utilized in the Smart Grid, especially in Home Area Networks (HANs) and Neighborhood Area Networks (NANs). Sensors can be used to monitor physical properties, such as temperature, lighting and humidity, and convert the observed information into electrical signals which will be forwarded to EMCS or other devices. Once EMCS receives the sensor signals, it will determine the signals and shed or shift electric loads in homes or buildings. Therefore, to ensure security, sensor nodes must be able to authenticate each other and verify that the signals received have not been tampered with by anyone. Regardless of what schemes will be implemented, keys and secret information must be used in order to ensure security goals. However, sensor nodes have resource limitations, such as slow CPUs, short battery life and small amounts of memory. Thus, the secret information that could be embedded in the sensor nodes is limited due to small memories. Also, keys could be distributed over-the-air, thus there must be mechanisms to protect the keys as well. One of the communication protocols that could be used in wireless sensor networks is Zigbee protocol. The most concern in the Zigbee-based HAN network is the process of setting up a new device in the network because an attacker could connect his device in the Zigbee as well. Another issue is 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. 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 key is sent over-the-air in plaintext, which is susceptible to one-time eavesdropping attack.
- Key Transport is to have a 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. Thus, 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 a trust center and devices negotiate the keys without transporting the key itself. Key Agreement is the most secure method for key establishment between devices in the network²⁵. 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, since it has to be pre-installed or sent over-the-air.

Even though, Zigbee provides mechanisms for key establishment and key distribution, it still has some of the security issues specified above. Thus, to implement wireless sensor networks in Smart Grid systems, those issues need to be solved beforehand.

25 R. Cragie, "Public Key Cryptographic in Zigbee Network", Dec 2008. [online]. Available: http://www.elektroniknet.de/fileadmin/user_upload/pdf/euzdc2008/Cragie_Jennic.pdf.

The research in this area should provide specific techniques or practices to protect the keys and also provide proper key management schemes that could be utilized in wireless sensor networks.

4.9 Side Channel Attacks

Cryptographic keys embedded into the equipment can be extracted using various attack schemes described in this section. Information obtained from these attacks is called side channel information and can facilitate extraction of the entire cryptographic key using this method. By carrying attacks based on timing measurements, power measurements, electromagnetic emission and faulty hardware side channel information can be retrieved.

Power analysis attacks

This kind of attack basically involves analysis of the power differences in the signal and converting the trace into logical zeroes and ones in order to extract the key.

Tempest attacks

This attack involves the principle that electronic devices such as monitors emit electromagnetic radiations during normal use. This can be obtained from a remote location using an antenna etc and replaying the information thereby invading privacy.

Timings attacks

In this type of attack the system is exploited by retrieving timing information which is obtained by examining the way in which inputs are processed by the system, including cryptographic keys.

Even though the side channel information does not provide complete information, but it provides enough information that can be amplified to analyze and extract keys. The research in this area is to come up with defense mechanisms that can be used to protect against those attacks.

4.10 Enhancing the Security of Serial Communication

Some legacy SCADA systems consist of serial communication links between the control centers and outstation devices. Most commonly used protocols on these serial links are DNP3 and modbus. They transmit text in unencrypted format and hence can be easily sniffed. Also solutions to enhance this such as wrapping protocols in IPSEC and SSL/TLS layer will put a load on these low bandwidth communication links and bring down the system speed to a large extent. This could impact the latency and bandwidth of communication and are not good solutions. Research is needed in order to find a mechanism which balances the speed of providing encryption and effect of encryption on the latency and bandwidth of the system.

4.11 Trust Management and Plug-in Hybrid Electric Vehicles

The Plug-in Hybrid Electric Vehicle (PHEV) network includes the vehicle owner's, utility (power generator) and retailer (power station similar to gas stations). There should be trust

between all the parties involved in the PHEV network. To establish this trust, each component in the PHEV network which includes the communication network, power meters and secure payment features, should undergo rigorous testing for security flaws in the PHEV system. With continuous R&D, a proper solution needs to be drawn.

Figure 4-2 shows the basic components in a PHEV network. R&D will need to find an appropriate solution for PHEVs.



Figure 4-2: Basic PHEV Networks

The components are individually listed below:

- 1) Smart Meter: This component of the PHEV is one of the most important and complex components. It performs the task of a power meter. It also has the ability to communicate with the smart grid (utilities or SCADA systems) and other vehicles.
- 2) Vehicle to Grid (V2G): Vehicle to Grid capability, in simple terms means the ability of a vehicle to provide power to, as well as receive power from the electrical grid.
- 3) Vehicle to Vehicle (V2V): Vehicular Communication Systems are an emerging type of networks in which vehicles and roadside units are the communicating nodes; providing each other with information, such as safety warnings and traffic information. As a collaborative approach, vehicular communication systems can be efficient in avoiding accidents and traffic congestions rather than each vehicle trying to solve these problems individually.
- 4) Communication: The PHEV network is a wireless mesh which uses protocols such as Zigbee, WiFi and 3G for long distance communication. There are 2 types of communication divisions; V2G, a long distance communication, where the PHEV directly interacts with the SCADA system or the utility and V2V which are short range communications, around 1/2 a mile in range. In this type of communication, each PHEV communicates with other vehicles within the range, to identify the traffic flow.
- 5) Demand Response (DR): DR signals in a PHEV network change very quickly and drastically, depending on the demand of power for charging the vehicles, the grid must generate more power or schedule the vehicles for charging, such that they are able to

adjust with the amount of power available. To perform these operations, a new system should be developed which can understand the demand and respond back to the vehicles by providing them power or scheduling an appropriate time. These systems are very complex and need to deal with real time demand response signals.

Figure 4-2 above shows the information flow between the different components of a PHEV network, each component must trust the information coming from the other component. An example would be best to explain the importance of trust in the PHEV network; for instance, if 1000 cars would start charging at the same instant, the grid would be unexpectedly overload, which may cause the grid to fail. To prevent the grid from overloading, a SCADA-like system could send a signal to the PHEVs to inform them when to start charging and when to stop. This system would thus schedule each PHEV's charging time. Another such instance could occur if an attacker uses a reply attack and send a signal to all the PHEVs instructing them to start charging. They would instantly start charging, causing the grid to fail due to the over load. These are just simple scenarios in the PHEV network where trust is very important. In the PHEV network information flows between the PHEV, utilities, power retails and the billing system. This information flow takes place in different networks using different protocols. Establishing trust in the information flow between different components of the PHEV network is one of the most important areas where research needs to be done. Some of the existing systems that can be examined for ideas on how to do this are as follows:

- Billing systems in the gas stations - these systems have been secured and well maintained, to be able to manage the third party involvements, gas station companies in this respect;
- Online banking systems - this system is generally secure as it ensures confidentiality, integrity and availability of the data to the authorized individuals,
- Information flow through cellular communications - this system has well implemented cross domain communications;

The above mentioned systems are examples of systems that have been developed and improved over the years. Research should be done to identify how these systems ensure such high level security with the goal of using similar security measures to enhance the PHEV security.

CHAPTER 5: Wireless Communication Security

5.1 Security for Routing Protocols in Wireless Mesh Networks²⁶

The two types of path determination (routing) techniques in wireless mesh networks (WMN) are proactive and reactive routing protocols. Proactive protocol is one which finds the path irrespective of the demand. Reactive protocols are those which find the path based on demand. There are threats associated with these routing protocols which might require knowledge about the routing protocols to inject erroneous packets to the network. The threats are summarized below:

Black-hole: An attacker creates forged packets to imitate a valid node in the mesh network. The packets are attracted by advertising low cost routes and further attacking by dropping the packets.

Grey-hole: Forged packets are used by the attacker to drop packets, route and inspect network traffic.

Worm-hole: Disruption of routing is carried out by replaying the routing control messages from one network location to another.

Route error injection: An attacker by injecting erroneous packets to the mesh network can break the mesh links.

These threats greatly depend on the routing technology used. A proprietary routing protocol is less susceptible to these kinds of threats when compared to routing protocol like Ad-hoc On-Demand distance vector (AODV). These risks could be reduced by implementing message integrity checking for the routing messages and device authentication. Also, the routers in a mesh network are typically not power constrained but the clients which are mobile are power constrained. Hence there is a need of efficient routing mechanism for WMNs.

Research in this area is to secure the routing protocols, as wireless mesh networks are integral part of Smart Grid communication networks.

5.2 IEEE 802.15.4 Security Issues²⁷

Asymmetric cryptographic algorithms like RSA and Diffie-Hellman use very long variables of sufficient length to ensure security. Sensor networks have very little memory and it is not sufficient to even hold these variables, let alone performing any operations on these variables. Also sensor networks have limited supply of energy. Hence the life span of a node is limited which in-turn limits the life span of a usable key. This hardware and energy constraint needs to

²⁶ A. Geriks, J. Purcell, "A Survey of Wireless Mesh Networking Security Technology and Threats", SANS Institute, September 2006.

²⁷ I. Ghansah, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, October 2009.

be addressed and more efficient solutions need to be designed keeping the above constraints in mind.

To minimize the memory constraint and ease the management overhead, network-wide shared keying method was introduced. Here all the nodes in a network use a single key to communicate with one another. This takes care of memory requirement. But the key management becomes a problem since if a single node in a network is compromised, an adversary could use the compromised node to undermine the security guarantees of the entire network.

To avoid the problem with network-wide shared keying method, pair-wise keying was introduced. Here, pair of nodes in a network uses a unique key to establish a secure communication, this leads to management and memory overhead. As the number of nodes increase, each node's memory requirement and key management ability will also need to be upgraded.

A low cost solution to the keying methods discussed above was provided with a trade-off between network-wide shared keying and pair-wise keying, with partial resistance to node compromise. Here a common key was used to establish secure communication between a set of nodes belonging to a group. These nodes are grouped based on the location, network topology and other similar functions.

The above mentioned solutions are summarized by the following examples:

- 1) If a key is used in multiple ACL entries then it is likely to reuse a nonce value (unique key used for encryption), in which case confidentiality can easily be broken. For example, if a user sends a message m_1 with a nonce value x_1 to recipient r_1 and then sends a message m_2 with the same nonce value x_1 to recipient r_2 , the adversary can retrieve the message as show below²⁸.

$$(m_1 \oplus E_k(x_1)) \oplus (m_2 \oplus E_k(x_1)) = m_1 \oplus m_2$$

where E_k denotes encryption of the data using key k

- 2) Network-wide shared key is incompatible with replay protection. For example, if user A sends 100 messages to recipient r_1 , the replay counter would be incremented from 0 to 99 at the receiver's end. Now if user B sends a message to recipient r_1 with a replay counter 0, the recipient r_1 rejects the message as its replay counter has been incremented and is no longer 0. Recipient r_1 would only accept a message from user B if the replay counter value of the message is greater than 99. To overcome such issues, there has to be some form of co-ordination between the nodes in the replay counter space. This would not be feasible when the node density increases.

Thus working on finding a solution that would solve the problem of the ACL tables' inability to support different keying models is required in IEEE 802.15.4.

²⁸ N. Shastry, D. Wagner; UC Berkley., "Security Considerations for IEEE 802.15.4 Networks", Year of Publication - 2004.

GLOSSARY

ACL	Access Control List
AIK	Attestation Identity Key
AMI	Advance Meter Infrastructure
AODV	Ad-hoc On-Demand distance vector
CA	Certificate Authority
CEK	content-encryption key
CIAS	Center for Information Assurance and Security
CRL	Certificate Revocation List
CRT	Chinese Remainder Theorem
DAA	Direct Anonymous Attestation
DH	Diffie-Helman
DoS	Denial of Service
DR	Demand Response
DSS	Digital Signature Standard
ECC	Elliptic-Curve Cryptography
EK	Endorsement Key
EMCS	Energy Management Control System
HAN	Home Area Networks
IBE	Identity based encryption
IDS	Intrusion Detection Systems
IED	Intelligent Electronic Devices
NAN	Neighborhood Area Networks
PHEV	Plug-in Hybrid Electric Vehicles
PKG	Private-key Generator
PKI	Public Key Infrastructure
PPS	Public Parameter Server
RA	Registration Authority

RBAC	Role-Base Access Control
SCADA	Supervisory Control and Data Acquisition
TPM	Trusted Platform Module
WSN	Wireless Sensor Networks

REFERENCES

- I. Ghansah, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, October 2009.
- I. Ghansah, "Best Practices for Handling Smart Grid Cyber Security", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, February 2010.
- D. Andert, R. Wakefield, and J. Weise, Professional Service Security; Sun Microsystems Inc., "Trust Modeling for Security Architecture Development", December 2002 [online]. Available: <http://www.sun.com/blueprints/1202/817-0775.pdf>
- M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs – Research, A. Keromytis; U. of Pennsylvania, "The KeyNote Trust-Management System Version 2", September 1999 [online]. Available: <http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt>
- M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs – Research, A. Keromytis; U. of Pennsylvania, "The KeyNote Trust-Management System Version 2", September 1999 [online]. Available: <http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt>
- I. Ghansah; California State University Sacramento, D. Thanos; GE Digital Energy, P. Pal, and R. Schantz; BBN, C. Gunter, T. Yardley, and Himanshu Khurana; University of Illinois, E. Berozet; Elster, S. Klein; OSECS, R. Jepson; Lockheed Martin, J. Ascough, and R. Henning; Harris Corp. P. Blomgren; SafeNet, G. Emelko; ACLARA Tech, K Garrard; Aunigma Network Security Corp, "R&D Themes for Cyber Security in the Smart Grid", March 25, 2010 [online]. Available: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGRandD/RDIdeas-March30_2010.doc
- A. Lee, T. Brewer; The Cyber Security Coordination Task Group, "DRAFT NISTIR 7628 - Smart Grid Cyber Security Strategy and Requirements", September 2009 [online]. Available: <http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf>
- M. Enstrom, "(DRAFT) Privacy Chapter Introduction", April 06, 2010 [online]. Available: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628PrivacyIntroApr2010>
- A. Arsenault; Diversinet, S. Turner; IECA, PKIX Working Group, "Internet X.509 Public Key Infrastructure: Roadmap", July 2002 [online]. Available: <http://tools.ietf.org/html/draft-ietf-pkix-roadmap-09>
- National Institute of Standard and Technology (NIST), "Digital Signature Standard (FIPS 186-3)", June 2009 [online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.
- E. Stavrou, "PKI: Looking at the Risks", January 2005 [online]. Available: <http://www.devshed.com/c/a/Security/PKI-Looking-at-the-Risks/>

- E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
- G. Appenzeller, L. Martin; Voltage Security, M. Schertler; Tumbleweed Communications, "Identity-based Encryption Architecture", Internet Draft, November 2007 [online]. Available: <http://tools.ietf.org/html/draft-ietf-smime-ibearch-06>
- M. Gagné, "Identity-Based Encryption: a Survey", RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003
- Identity based encryption, Russell Kay Computer world Nov 17th 2008
- A White Paper by Vertoda, "An Overview of Identity Based Encryption", 2009 [online]. Available: <http://www.slideshare.net/vertoda/an-overview-of-identity-based-encryption>
- G. Appenzeller; Stanford University, L. Martin; Voltage Security, M. Schertler; Axway, "Identity-based Encryption Architecture and Supporting Data Structure", January 2009 [online]. Available: <http://tools.ietf.org/search/rfc5408>
- WikiPedia, "Trused Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module
- WikiPedia, "Trused Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module
- S. Bajikar; Mobile Platform Group, Intel Corporation, "Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper", June 20, 2002 [online]. Available: http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf
- TPM specification, version 1.2, Revision 103. http://www.trustedcomputinggroup.org/resources/tpm_main_specification
- P. Kitsos, O. Koufopavalou, G. Selimis and N. Sklavos VLSI Design Lab, Electrical and computer dept, University of Patras Rio, 26500 Patras, Greece, "Low power cryptography", [online]. Available: http://iopscience.iop.org/1742-6596/10/1/084/pdf/jpconf5_10_084.pdf?ejredirect=migration
- J. Fox, B. Gohn, C. Wheelock, "Networking and Communications, Energy Management, Grid Automation, and Advanced Metering Infrastructure", PIKERESearch, 4Q 2009.
- K. Gill, S. Hua Yang, F. Yao, and X. Lu; IEEE Transactions on Consumer Electronics, "A ZigBee-Based Home Automation System", Vol. 55, No. 2, May 2009 [online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05174403>

- E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available:
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
- R. Cragie, "Public Key Cryptographic in Zigbee Network", Dec 2008. [online]. Available:
http://www.elektroniknet.de/fileadmin/user_upload/pdf/euzdc2008/Cragie_Jennic.pdf
- A. Geriks, J. Purcell, "A Survey of Wireless Mesh Networking Security Technology and Threats", SANS Institute, September 2006.
- I. Ghansah, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, October 2009.
- N. Shastry, D. Wagner; UC Berkley., "Security Considerations for IEEE 802.15.4 Networks", Year of Publication – 2004.