TAMPERE UNIVERSITY OF TECHNOLOGY

KIM PAANANEN

INFORMATION SECURITY IN SMART GRID DEMONSTRATION ENVIRONMENT

Master of Science Thesis

Examiner: Professor Hannu Koivisto
Examiner and topic approved in the Automation, Mechanical and Material Engineering Council meeting on 7th of December 2011

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Automaatiotekniikan koulutusohjelma
PAANANEN, KIM: Tietoturvallisuus Smart Grid -demonstraatioympäristössä
Diplomityö: 97 sivua, 10 liitesivua
Maaliskuu 2012
Pääaine: Automaatio- ja informaatioverkot
Tarkastaja: Professori Hannu Koivisto
Avainsanat: Smart Grid, älykäs sähköverkko, tietoturvallisuus

Jatkuva maapallon väkiluvun ja energiatarpeen kasvu ovat johtaneet maailman energiakriisiin. Vanhat energialähteet ovat käymässä vähiin ja siirtyminen uusiutuvien energiamuotojen käyttöön on alkanut. Nykyinen sähköverkko on tehoton ja vanha eikä pysty täyttämään nykypäivän vaatimuksia. Yhtenä vaihtoehtona näiden ongelmien ratkaisemiseen on hyödyntää kaksisuuntaista sähkön ja informaation kulkua, jota kutsutaan myös Smart Gridiksi. Koska Smart Grid hyödyntää informaatio- ja kommunikaatioteknologioita, altistuu se myös tietoturvauhkille. Smart Grid koostuu useista osajärjestelmistä luoden monimutkaisen automaatioympäristön. Smart Gridin turvaaminen on tästä syystä hankalaa, mutta pakollista, sillä onnistuneiden hyökkäysten seuraukset voivat olla katastrofaalisia. Tämä diplomityö on osa CLEEN SHOK Smart Grids and Energy Markets -projektia tutkien Smart Grid -demonstraatioympäristön tietoturvallisuutta. Työn päätavoitteina ovat analysoida ja testata Smart Grid -implementaation tietoturvallisuutta ja luoda tietoturvatarkastuslista eri yrityksille, jotka toimivat Smart Grid -ympäristössä.

Tämä diplomityö on jaettu neljään osaan. Kirjallisuustutkimuksessa esitellään tietoturvallisuuskäsitteitä ja -ympäristöä sekä Smart Gridiä yleisellä tasolla. Tämä vaihe tutustuttaa lukijan myös Smart Grid -käsitemalliin sekä -demonstraatioympäristöön. Analyysivaiheessa demonstraatioympäristöä eritellään uhkamallinnusta käyttäen ja tutkien demonstraatiolaitteita tarkemmin. Uhkamallinnus on tehty asiakkaan näkökulmasta ja se tarjoaa korkean abstraktitason analyysin, siinä missä demonstraatiolaitteiden tarkastelu tarjoaa syvän, laitteistoläheisen analyysin. Testausvaiheessa demonstraatiolaitteisto testataan ja testauksen tulokset esitetään. Tämä vaihe sisältää testaussuunnitelman ja siinä käytettävät testausohjelmat. Viimeisessä osassa esitetään tarkastuslista. Tämä tarkistuslista tarjoaa 10 parasta kriittistä tietoturvakontrollia, mitkä soveltuvat erityisesti kotiautomaatioympäristöön.

Tutkimus osoittaa, että demonstraatioympäristö sisältää tietoturvapuutteita. Yleisimmät haavoittuvuudet johtuvat ohjelmien vääristä asetuksista sekä versioista, jotka sisältävät tietoturvauhkia. Demonstraatioympäristön tärkein osa on ThereGate, joka on myös kuluttajien käyttöliittymä Smart Gridiin. Kyseinen laite sisältää monta vakavaa tietoturvaongelmaa, jotka täytyy korjata. ThereGaten suojaaminen on oleellisen tärkeää koko systeemin toimivuuden ja turvallisuuden kannalta.

Smart Gridin luotettavan toiminnan turvaaminen vaatii tietoturvallisempia menettelyjä, kuten asiakkaan vahva tunnistaminen. Niin kauan kuin standardit pelkästään suosittelevat eivätkä pakota tietoturvamekanismien käyttöä, kuten tiedon salaamista, ei niitä käytetä. Työn tuloksena voidaan sanoa Smart Gridin luotettavan toiminnan varmistamisen vaativan lisää toiminnan luotettavuuteen tähtäävää tietoturvatutkimusta.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Program in Automation Technology
PAANANEN, KIM: Information security in Smart Grid demonstration environment
Master of Science Thesis: 97 pages, 10 appendix pages
March 2012
Major: Automation and information networks
Examiner: Professor Hannu Koivisto
Keywords: Smart Grid, smart electric grid, information security

The ever growing population and need for energy has culminated in an energy crisis. Old, traditional energy sources are running low and the transition to renewable ones has begun. The electric grid, however, is very old, being inefficient and incapable of meeting the needs of today. One solution for these problems is to utilize a two-way flow of electricity and information, also known as Smart Grid. As Smart Grid utilizes information and communications technology, it will be exposed to information security threats. Smart Grid comprises of many systems, creating a complex automation environment. Thus, even if making Smart Grid secure is troublesome, it is essential to ensure its security since the consequences of successful attacks can be disastrous. This thesis is part of CLEEN SHOK Smart Grids and Energy Markets project and studies the information security of the Smart Grid demonstration environment. The main goals are to analyze and test the information security of the Smart Grid implementation, and to generate a best practice information security checklist for different players in the Smart Grid environment.

The thesis is divided into four phases. In the literature study the focus is on information security landscape and features, as well as Smart Grid on general level. This phase includes a presentation of the conceptual model of Smart Grid and the demonstration environment on a general level. In the analysis demonstration environment is analyzed through threat modelling and closer examination of the demonstration equipment. The threat model works from the customer´s point of view, concentrating on home energy management system, and providing high abstract level analysis, whereas the examination of the equipment provides more specific analysis. In the testing, the demonstration environment is tested, and the results are presented. This phase also includes the testing layout and introduces the software used for the testing. The final section focuses on generating a best practice security list. This checklist provides the top 10 critical controls of information security for the Smart Grid environment, especially for a home automation environment.

In the course of the study, it is indicated that the information security of the demonstration environment has shortages. The most common vulnerabilities are due to wrong software configurations, and using vulnerable versions of software. The most critical part of the demonstration environment is the end user's device, which in this study was ThereGate. This equipment has many security issues that need to be taken care of. Securing ThereGate is essential in regard to the entire system's dependability and security.

To secure dependable Smart Grid, stronger methods like strong client authentication are required. As long as standards only recommend and do not require information security methods, like encryption, they will not be used, and thus, they will make the system more vulnerable. As a result, it can be said that more security research is required in order to secure a dependable Smart Grid.

PREFACE

This document is a part of my work graduating as Master of Science in Automation Engineering from Tampere University of Technology. This master's thesis has been done for the Department of Automation Science and is part of a larger EU project. I would like to thank all companies that were behind this project and especially, Codenomicon Oy, who provided the testing software. I would also like to thank my examiners, researcher Jari Seppälä and professor Hannu Koivisto, for comments and interesting conversations. Last but not least, I would like to thank my dear family and friends for the given support.

Tampere, March 2012

Kim Paananen

CONTENT

1 Introduction 1
2 Information security 3
2.1 Landscape 3
2.2 Definition and objectives 4
2.3 Special information security features of Smart Grid 6
2.4 Threats 7
2.4.1 Attacks 7
2.4.2 Adversaries 8
2.4.3 Vulnerabilities 10
2.5 Security measures 11
2.5.1 Cryptography, identification and authentication 11
2.5.2 Technical solutions and methods 13
2.6 Security testing techniques 14
3 Smart Grid 16
3.1 The landscape 16
3.2 Infrastructure and architecture 17
3.3 Benefits 20
3.4 Players 20
3.5 The conceptual model 22
3.5.1 Domains and actors 23
3.5.2 Differences between North America and Europe 26
3.6 Smart Grid demonstration environment 27
3.6.1 Use cases 28
3.6.2 The domains, actors and players 28
3.6.3 Laboratory demonstration equipment 31
4 Applied threat modeling 32
4.1 The scope and limitations 32
4.2 Viewing the system as an adversary 33
4.2.1 Entry and exit points 33
4.2.2 The assets 35
4.3 Characterizing the system 36
4.3.1 Implementation of the system 38
4.4 Determining threats and vulnerabilities 39
4.4.1 HEMS crashes 39
4.4.2 HEMS works incorrectly 40
4.4.3 HEMS losses sensitive information 43
5 Review of laboratory demonstration 44
5.1 Components 44
5.1.1 ThereGate 45
5.1.2 Aggregator 46

5.1.3 Industrial control system 48
5.2 Information security analysis 49
5.2.1 Vulnerabilities in hardware 49
5.2.2 Vulnerabilities in software 50
5.2.3 Vulnerabilities in protocols and communication technologies 51
6 Detailed analysis and test results 53
6.1 Test case analysis 53
6.1.1 Customer owns ThereGate 53
6.1.2 ISP owns ThereGate 54
6.1.3 DSO owns ThereGate 55
6.1.4 Conclusion 56
6.2 Testing plan 56
6.2.1 Target and layout 56
6.2.2 Used tools 57
6.2.3 Testing methodology 59
6.2.4 Execution of testing 61
6.3 Testing results 61
6.3.1 Open ports and services 62
6.3.2 Version of software 65
6.3.3 Software configuration 66
6.3.4 Information disclosure 67
6.3.5 Protocol flaws 69
6.3.6 Encryption of information 71
6.3.7 Authentication 72
6.3.8 Other found issues 74
6.3.9 Synopsis of the test results 74
7 Best practices Security check list 76
7.1 Customer Domain – HEMS/Home automation: 76
8 Conclusion 84
References 85

Appendix A I
Appendix B IV
Appendix C VII

TERMS AND DEFINITIONS

3G	3rd generation mobile telecommunications.
Aggregator	An aggregator is a centralized information source quite like SCADA, that aggregates information from various sources.
AMI	Advanced Metering Infrastructures are systems that measure, collect, and analyse energy usage and communicate with metering devices.
Anonymous	Name for famous hacker or hacktivist group.
ANSI	American National Standards Institute.
API	Application Programming Interface is a language and message format that software programs can use to communicate with the operating system or some other control program. It is an interface between different software programs.
ARP	Address Resolution Protocol is used for matching IP addresses to MAC addresses, when IP protocol is used.
BAN	Building Area Network is a network in customer premises connecting devices to each other. A type of LAN.
Blowfish	Blowfish is a strong symmetric block cipher. The key length varies from 32 bits to 448 bits.
C12.22	C12.22 is the American National Standard for Protocol Specification for Interfacing to Data Communication Networks.
CA	Certificate Authority, an entity that issues digital certificates.
CIA	Central Intelligence Agency.

CIA	Confidentiality, integrity, and availability. The core principles of information security.
CM	Configuration Management.
CPU	Central Processing Unit
CSIv2	Common Secure Interoperability Version 2
CSRF	Cross-site request forgery is an attack, which forces an end user to execute unwanted actions on a web application in which she or he is authenticated.
DCS	Distributed Control Systems.
DES	Data Encryption Standard, a block cipher that uses shared secret encryption. The length of the block is 64 bits and key length is 56 bits. Due the length of the key, DES is not used widely anymore. Triple-DES has taken its place.
DLMS/COSEM	Device Language Message specification/Companion Specification for Energy Metering is the common language of Automatic Meter Reading, or Demand Side Management.
DMS	Distribution Management System is a collection of applications used to monitor, and control the distribution power system reliability, and efficiency.
DMZ	Demilitarized zone is an information security method. It is physical or logical subnetwork that connects company´s external services to entrusted network.
DNS	Domain Name System is a naming system for computers, services or other resource connected to the network. It changes hostnames into IP addresses.
DoS	Denial-of-service is a situation, where resources and services are unavailable to intended users.

DSO	Distribution System Operator operates the distribution systems, which purpose is to distribute power from the transmission network to customers.
DSR	Demand Side Response is a modification of consumer demand for energy. The goal is to encourage consumers to use less energy during peak hours, or move the use of energy to off-peak times.
Easter Eggs	Intentionally hidden information, such as pictures.
EMS	Energy Management System is a system of computer-aided tools used by operators of electric utility grids to monitor, control, and optimize the performance of the generation and/or transmission system.
ESI	Energy Service Interface is the primary service interface to the Customer domains, and it communicates with other domains via the AMI infrastructure, or via, for example, the Internet. It provides a secure interface for Utility-to-Consumer interactions, and can act as a bridge to facility-based systems, such as the customer's energy management system.
EU	European Union.
FAN	Field Area Network is a network that includes devices communicating between the individual service connections, and backhaul points leading to the utility. It also includes distribution automation and control devices.
GPRS	General Packet Radio Service is a packet oriented mobile data service that works in GSM network.
GSM	Global System for Mobile Communications is a global cellular network.
GUI	Graphical UI is a type of user interface that uses images instead of text commands to interact with users.
HAN	Home Area Network is a network in customer premises connecting devices to each other. A type of LAN.

HEMS	Home Energy Management System is an interface for customer resources as well as UI for customers to Smart Grid. It includes both ESI, and customer´s ESM.
Home PNA	Is a technology for home networking over the existing coaxial cables and telephone wiring.
HTTP	Hypertext Transfer Protocol is a networking protocol used by the WWW for the data communication. It defines how Web servers and browsers should respond to various commands, and how messages are formatted and transmitted.
HTTPS	Hypertext Transfer Protocol Secured is a combination of HTTP and SSL/TLS protocols used for secure transmission of information.
ICMP	Internet Control Message Protocol is one of the core protocols of the TCP/IP.
ICS	Industrial Control System is a general term that encompasses several types of control systems, such as SCADA and DCS systems.
ICT	Information and Communication Technology is a system consisting of equipment and networks, which are used to treat information.
IDEA	International Data Encryption Algorithm is a symmetric block cipher. It operates on 64 bit blocks using 128 bit key.
IDS	Intrusion Detection System is a system that monitors the network, looking for suspicious behaviour, and alerting of an attack.
IEC	International Electrotechnical Commission
IP	Internet Protocol is the principle communications protocol, which takes care of transmitting packets.

IPS	Intrusion prevention system is network security software that monitors the network and system for malicious activity.
IPSec	A security protocol that authenticates and/or encrypts each IP packet.
ISO	Independent Systems Operators is an organization that controls and monitors the operation of the electrical power system within a single or multiple states in USA.
ISP	The Internet Service Provider is a company that provides access to the Internet.
IT	Information Technology is a system that handles information.
JDBC	Java Database Connectivity is an interface that defines a way in which customers can use a database.
JSON	JavaScript Object Notation is a lightweight data-interchange format, which is easy for humans to read and write, and easy for machines to parse and generate.
LAN	Local Area Network is a computer network covering a small physical area.
LTE	Long Term Evolution is evolution of 3G technology.
LV	Low Voltage. Less than 1 kV.
MAC	Message Authentication Code is a unique hardware address that identifies each node of a network.
M-Bus	A light-weight local coordination protocol providing a simple and flexible message oriented communication channel for a group of components.
MID	Measuring Instrument Directive.
MITM	A man-in-the-middle attack is one in which the adversary intercepts communications between two parties.

MOF	Managed Object Framework
MV	Medium voltage. Less than 50 kV.
ANSI C12.18	ANSI C12.18 is an ANSI standard that describes a protocol used for two-way communications with an electricity meter. Used mostly in North America.
NAT	Network Address Translation. A process of modifying IP address information in IP packet headers, while in transit across a traffic touring device.
NE3S/WS	Nokia Enhanced SNMP Solution Suite/Web Service.
NIST	National Institution of Standards and Technology
OCoS	Open Configuration Data Standard.
OES	Open EMS Suite is an element management system (EMS) platform product providing operation and maintenance interface solutions.
OMeS	Open Measurement Standard.
OPC UA	OPC Unified Architecture is the most recent OPC specification.
OPC	Openness, Productivity, and Collaboration is an open source data transfer standard, which is used in automation systems.
OS	Operating System.
OSI- model	Open System Interconnection Reference Model
PAN	Premise Area Network is a network in customer premises connecting devices to each other. A type of LAN.
PGP	Pretty Good Privacy is a computer program that provides more security by public key encryption and authentication. It is used, especially, with E-mails.

PHP	Hypertext Preprocessor is a programming language used especially in Web server environment.
PKI	Public Key Infrastructure is a digital certificate scheme.
PLC	Power Line Communication is a data transmission system that uses the existing power lines within a home, building, or an outdoor power distribution network.
PM	Performance Management.
RC4	RC4 is a widely used symmetric encryption algorithm.
RC5	RC5 is a simple block cipher.
RF	Radio Frequency
S/MIME	Secure/Multipurpose Internet Mail Extension is a standard, which defines encryption and signing of e-mails by using public key cryptography.
SAN	Substation Area Network is a network that includes devices such as capacitor banks and relays, communicating inside a single electric substation.
SANS	SANS is an institute that is most trusted, and by far the largest source for information security training, and security certification in the world
SCADA	Supervisory Control and Data Acquisition refers to the automation system used to monitor, and control industrial process
SGEM	Smart Grid for Energy Market
SGWC	Smart Grid Working Croup
SOAP	Simple Object Access Protocol is a protocol specification for exchanging structured information in Web Services.
SPKI	Simple Public Key Infrastructure is a specification for digital certificate scheme.

SQL	Structured Query Language is a programming language designed for managing data.
SSH	Secure Shell is a network protocol for secure data communication, remote shell services, or command execution.
SSL	Secure socket layer is a cryptographic protocol that provides security for communications over networks such as the Internet.
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol is the set of communication protocols used for the Internet. The name comes from the most important protocols in the set: Transmission Control Protocol / Internet Protocol.
TLS	Transport Layer Security is a cryptographic protocol that provides security for communications over networks such as the Internet.
TNS	Transparent Network Substrate is an Oracle computer networking technology for peer-to-peer connectivity.
TPM	Trusted Platform Module is a secure cryptographic processor that offers secure generation and storing of cryptographic keys, and limitation of their use.
Triple-DES	Triple Data Encryption Algorithm is a block cipher that uses DES cipher algorithm three times to each data block.
TSO	Transmission System Operator is a non-commercial organization – usually at least partly owned by the state or government – responsible for an area to be electrically stable, and for the security of supply in this area.
UDP	User Datagram Protocol is one of the core protocols of the TCP/IP.
UI	User Interface is a place where interaction between human and computer occurs.

UPnP	Universal Plug and Play is a set of networking protocols, the purpose of which is to make different kinds of equipment to work easily together.
VLAN	Virtual Local Area Network is a group of hosts with requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location.
VPN	Virtual Private Network is a way for combining two or more networks into a private network over a public network.
WAN	Wide Area Network is a computer network that covers a broad area.
WLAN	Wireless Local Area Network.
WPA	Wi-Fi Protected Access is security protocol used for securing wireless computer networks.
WS	Web Service is a method which enables the communication between two computers over network.
X.509	A standard for a PKI.
XML	eXtensible Mark-up Language is an open standard used for defining data elements on a WWW- document. Whereas HTML defines how elements are displayed, XML defines what they contain.
XSS	Cross-Site Scripting is a type of vulnerability that enables attacker to inject client-side script into web pages.
Z-Wave	A wireless communication protocol designed for home automation.

1 INTRODUCTION

The number of people, and moreover, the consumption of energy is increasing in an unstoppable manner. Covering this rise in demand with scarce, traditional, fossil based energy sources is a short sighted solution and only enhance the other big problem – global warming. This situation is forcing us towards energy efficient, and more ecological production as well as transmission of energy. In the last few years renewable energy sources, such as wind and solar power, have become a real option in energy production. However, the current electric grid is old and not planned or capable of utilizing renewable energy sources that well. One solution to these problems is a new electric grid called "Smart Grid", which changes the power generation from a centralized one to a decentralized one. Smart Grid modernizes today's one-way electricity delivering system into a highly automated and dynamic system by exploiting two-way flow of electricity and information. The layout of the Smart Grid is a multi-connected network instead of the more traditional tree model. However, as the new grid utilizes information technology (IT) and is more complex, it will be also exposed to new kinds of information security threats. Information security concerns are not restricted only to deliberate attacks but also situations such as natural disasters. The consequences of what might happen if an attacker penetrates a network can be severe. Thus, information security must be taken into account from the beginning into the very end.

This thesis studies information security in Smart Grid demonstration environment at Tampere University of Technology (TUT) and is a part of Smart Grid for Energy Market (SGEM). The SGEM is a CLEEN SHOK (Cluster for Energy and Environment/ Concentration of strategic top-level knowhow) program, and its objective is to create an innovation foundation for new solutions, products, and services to enable the implementation of the Smart Grid´s vision. The target of Task 6.2 is to ensure the dependability, integrity, confidentiality, and reliability of the new information and communications technology (ICT) architectures, and solutions for Smart Grid. The main goals of this thesis are to present a way of analyzing and testing information security of Smart Grid demonstration environment, and generate a best practice checklist for information security. The purpose of the checklist is to work as a tool on information security for different players, especially in the home automation environment of Smart Grid.

There are four phases in this thesis. The first phase, including chapters two and three, introduces the concept of information security in automation and presents Smart Grid on a general level, giving necessary background information to the reader. This phase also includes a presentation of the conceptual model of Smart Grid as well as the demonstration environment on a general level. The second phase, consisting of chapters

four and five, analyzes the demonstration environment through threat modeling and through a closer examination of the demonstration equipment. The threat model takes the customer´s point of view and concentrates on the home energy management system, providing high-level analysis, whereas the examination of the equipment provides more specific analysis. The third phase is the actual testing part where the demonstration environment will be tested using several different testing software. The testing and its results are performed in chapter six. The last phase of the thesis concludes the results in the form of a checklist for the best security practices. This checklist provides the top 10 critical controls of information security, especially for home automation environment and is presented in chapter seven.

2 INFORMATION SECURITY

The aim of this chapter is to give necessary background information on information security, especially in automation environments, such as Smart Grid. Defining the concept of information security with its objectives, as well as introducing the special needs of the automation system are vital for a deeper comprehension.

In this chapter, it will also be presented which kinds of threats, vulnerabilities, and attacks the digital world possesses, and who are the possible adversaries in Smart Grid environment. Other issues discussed include fighting against the adversaries´ attacks, security measures, and security testing techniques.

2.1 Landscape

Until recently, information security in automation systems, such as energy distribution systems, has been disregarded since there were no real threats to be considered. The environment was to a great extent closed and so the programs and protocols, that is everything, was designed for that environment. Nowadays however, the environment has changed from closed to open, and information security cannot simply be bypassed. Instead, it requires special attention and deep understanding. The consequences of what might happen if the automation system was hacked can be hazardous. [1, p. 152; 2, p. 28.]

There has also been a significant change in the hacking culture and procedures. Whereas hackers used to work alone, they now work as a group. In such a group one person can search for vulnerabilities, another can make exploits, and the next one can combine all these to one package while the last one uses the package to make money for all the participants. Nowadays, the systems are simply too complex for one individual to handle. For this reason, many hacking forums have been created where one can find information, join a group, or learn how to hack something. [3.] In addition the so-called normal and widely used virtual societies, such as YouTube [4], include a cornucopia of different tutorials for hacking.

Not only has the hacking culture changed but the tools for hacking have also evolved: there are now network discovery and vulnerability scanners, penetration tools, network monitoring tools, brute force tools, and social engineering tools that collect information from different public sources to create information packages from individuals, -and so forth. For some, it may seem surprising that one of these tools, a very powerful and used one, is Google. It can be used, for instance, to find vulnerabilities [5]. The motives behind the attacks vary from money to curiosity, and reputation to ideology. The denial-of-service- attacks (DoS), for instance, where the goal of the attack is to

make resources and services unavailable to users, are one way to blackmail money from companies. Hacking into companies' systems in order to find classified information has also grown [1, pp. 21-26].

Nowadays, people are more and more connected and attached to the Internet than ever before. Having a virtual-identity is almost a must, at least on some level. People are more careless in regard to what they publish about themselves in Internet societies, and what terms they agree with when joining. Following this progress closely, adversaries have adopted new ways to attack: social engineering, and phishing emails have become very common [3, p. 6]. Even if badly written emails may seem a cheap trick to fall into, many people still do. There is no overestimating the curiosity and general laziness of people.

Moreover, the amount of information gathered from each individual has grown a great deal. Facebook, for example, uses cookies in a way that enables them to track the pages that a subscriber visits, even when logged out [6]. Third party service providers, however, are not the only ones to track people´s actions – governments do it as well. Every laser printer, for instance, leaves a unique trace that can be used to track down the owner of the printer if necessary. Although this may seem harmless, especially to people who have nothing to hide, it is a matter of freedom against control. [7.] The recent incidents in Norway catalysed a conversation about the necessity of increasing surveillance online. However, giving more rights to the government is not necessarily the best solution from the citizen's point of view. This can be seen, for example, in China, where the government monitors and restricts Internet usage [8]. All this raises concerns about privacy, legislation, and consumer security. How much responsibility for information security can be left to end users, and can we trust the government of today and the one of the future?

An important part of Smart Grid will be the new technological solution that can be used to improve the system. These technologies are important but also increase the attack surface of the system. For example, as the electric cars implement operating systems (OS) and applications [9], they can be used to gain access to the network of the local electricity supplier via, for instance, a car´s battery system. Additionally, devices such as smart phones, will be involved in more attacks either as a target, or as a means to access another system. These factors shape the landscape of information security in Smart Grid to a very complex and vast one.

2.2 Definition and objectives

One issue worth clarifying is the concept of information security. There exists a myriad of opinions and beliefs of what information security is, and it is often seen only as a technical solution. Information security is, nevertheless, much more than a personal firewall.

The environment of Smart Grid is not a simple IT environment, but instead, a complex automation environment. Thus, the information security of Smart Grid follows

closely the information security of automation. Information security of automation is, most of all, a part of availability [10]. It is used for preventing unplanned disruptions, and to guarantee availability. Information security is a vast field, and it cannot always be defined to cover all parts [11, pp. 27-28]. Described in Figure 2.1 is one definition of information security in automation.

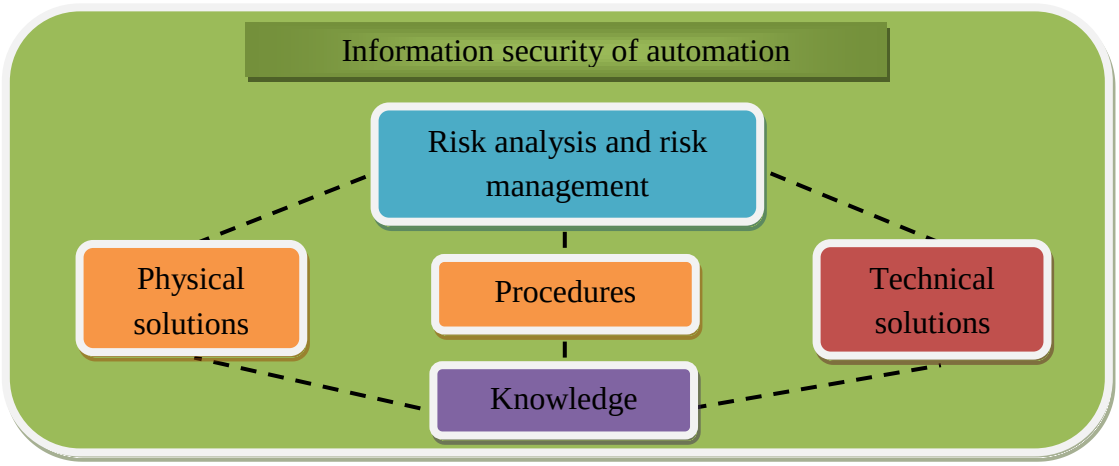

Figure 2.1. *The building blocks of information security in automation [10].*

In the end, information security can be seen as risk management, where the safety level required for the desirable level of availability is defined. In other words, with safety management it can be explained why a certain safety level of security has been chosen. Physical solutions are the foundation of technical solutions; if there is no physical safety, technical safety solutions are easy to bypass. On the other hand, many companies rely plainly on physical safety; if an attacker can penetrate the physical obstacle, it will have access to the company's network. Technical solutions are the defence against network attacks and against disruptions caused by users or operation systems. Procedures, that is the way people do things, are user interfaces (UIs) to information security. Knowledge is internal information security, and it is gained through education. It supports the use of tools. Procedures, as well as technical and physical solutions, are tools for safety management. [10.]

Smart Grid is a complex system, combining many different sub systems. The two most important sub systems in regard to information security are the power and ICT systems. In the power system, the most important factors are availability and reliability, which depend mostly on information security and functional safety. In ICT systems, information security focuses on ensuring the confidentiality, integrity, and availability (CIA) of the system. These have been derived from the fact that ICT systems in general, treat data, meaning there are only three ways that a computer can fail [12, p. 149]:

1. The computer does not deliver the data on which we are dependent
2. The computer delivers data with an erroneous value
3. The computer delivers data to someone who is not authorized to receive those data

Information security in the Smart Grid must take into account the combined requirements of both, power and ICT systems. The objectives of information security for Smart Grid are ensuring the availability of the grid, and ensuring the integrity and the confidentiality of the information. [13, p. 4; 14, pp. 35-45.] The objectives are described below in Figure 2.2.

Figure 2.2. *The objectives of information security in Smart Grid.*

These objectives identify the special structure of the Smart Grid: availability stands for the needs of the automation system, integrity for the ICT system, and confidentiality for the customer oriented system.

One important part of confidentiality is customer privacy. This subject is being studied under work package four in sub task 10 of the SGEM project. Thus, in this thesis, privacy is left in the background.

2.3 Special information security features of Smart Grid

The special features of automation, such as real time-operations, limited processing power, and the continuity of the process have to be taken into account, especially when identifying the security requirements. The security requirements define what safety measures and technical solutions are to be used in order to assure the continuity of the process. In regard to the automation environment, following characteristics must be considered [11, pp 15-16]:

- The consequences of a disruption can be severe
- The lifespan of an automation system is long
- Automation systems usually use custom made programs
- Different user groups
- Multivendor facilities

For example, since the lifespan of an automatic system is long, updating system components can be hard; OSs are so old that no security updates are available. In addition, combining different information systems may cause problems. [1, pp 19-20.]

There are also differences between the so-called normal process automation system and a Smart Grid system. First of all, Smart Grid will be strongly distributed and widely spread geographically speaking. Additionally, there are several interaction points to other systems and parties involved. All parties have to have necessary information about

the process, and usually data transfer is done via some public network, such as the Internet. In order to gain a good level of information security in this environment, there needs to be a consensus about the responsibilities, and the special features of each automation system that must be taken into account. [11, pp. 127-140.] However, as the Smart Grid consists of so many parties and so many systems, gaining the necessary level of information security is somewhat challenging.

2.4 Threats

The threats in the digital world are those of the physical world; if physical banks are robbed, so the digital ones will be too. Theft, racketeering, vandalism, voyeurism, exploitation, extortion, con games, fraud, and anything can be similarly done in the digital world, only the methods are different. Whereas in the physical world they use lockpics, in the digital one they use manipulation of connection and databases. [15, pp 15-16.] Where there is enough money or something worth money, for instance information, there will be those who try to take advantage of it.

The digital world, however, has features that make it even more attractive and suitable for criminals: automation, omnipresence of Internet, and technique propagation. An adversary could, for example, take money illegally from a person´s bank account at any place in the world and at any time by using an automated script. Because of these features, it will be harder to track, capture, and convict the perpetrators. It may, for instance, be impossible for the prosecution authorities in one country to arrest a criminal in another country. Thus, the attacks will be much more common and larger scale than in the physical world. Even now, it is probable that the number of Internet crimes is bigger than physical ones. [15, pp. 17-22; 16.]

Smart Grid is a complex system of systems, and thus the threats depend on what kind of environment the company is working in. However, on many occasions, the system is based on the usage of public networks, such as the Internet, and on the usage of web technologies (see chapter 6.1). Thus, web based threats are, in many cases, relevant. [17.] The most common threats are injection flaws, cross-site scripting (XSS), weak authentication and session management, insecure object references, cross-site request forgery (CSRF), and poor security configuration. XSS is a situation where an attacker is able to inject client-side script into web pages, whereas in CSRF an end user is forced to execute unwanted actions on a web application in which she or he is authenticated. [18].

2.4.1 Attacks

The most common types of network attacks are eavesdropping, data modification, identity spoofing, password-based attacks, DoS attacks, man-in-the-middle (MITM) attacks, compromised-key attacks, sniffer attacks, and application layer attacks [19]. Probably the most dangerous of all attacks is a MITM attack, in which the adversary takes over the control of the network traffic. This way, the adversary can attack the field devices

unnoticed, by sending normal operational data to operator. [20.] In DoS attack, the idea is to send so much data to the target that it shuts down and makes the service – provided by the target – unavailable. There are many variations of this, but the basic idea is the same. In a case of distributed denial-of-service (DDoS) attack, the sources of the attack come from many different places. [11, p. 23-24; 15, pp. 181-186.]

One way to categorize these attacks is to divide them into three classes: criminal, publicity, and legal attacks. Criminal attacks are probably the most obvious, and easy to understand, whereas publicity and legal attacks can be much more damaging. [15, p. 23.]

Criminal attacks aim at making a profit. The types of attackers can vary a great deal from lonesome riders to organized crime groups; from insiders to governments. The types of attacks can be, for example, fraud, scam, destructive attacks, intellectual property theft, identity theft, and band theft. Privacy concerns form another issue. Different countries have different laws on them, some more strict than others. Privacy violations can be used for criminal purposes, but also legal ones. The difference between legal and illegal is a matter of technique used in the process. There are two types of privacy violations – data harvesting and targeted attacks. [15, pp. 23-41.]

The attacks that are done in order to get publicity are called publicity attacks. These kinds of attacks are harder to figure out and are still relatively new in the digital world. Typically, the attackers are skilled hackers and choose their target system based on the probability that the press will cover it. [15, pp. 23-41.] One very widely used attack for publicity purposes is the DoS attack.

The legal attacks are fundamentally different from the others in that their idea is not to exploit a flaw, or even trying to find it. The idea is to put doubt in the minds of the judge and jury of the fact that the security is not perfect, and to use this observation to prove the client's innocence. [15, pp 23-41.]

2.4.2 Adversaries

Behind every attack, directly or indirectly, is a human being or a group of people. They are fundamentally the same as in the physical world. However, locating the origin of the attack can be harder and in most cases even impossible in the digital world. Finding associates is also much easier in the digital world as one can stay home and keep one´s anonymity. Different adversaries have different objectives, motives, resources, levels of access and so on. The motives behind the attacks vary, most typical ones being vandalism, curiosity, social pressure, challenge, thoughtlessness, and easiness. [15, pp. 42-43.] Recently, there has also been a change in the types of attackers; whereas the attackers used to be relatively random and amateur, they are now organized and professional. [11, p. 59.]

Table 2.1. *The list of adversaries that NIST – SGWC introduces [13, p. 20].*

Adversary	Description
Nation States	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, which is normally not well organized or financed. Normally consists of few individuals, or of one individual acting alone.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or Poorly Trained Employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another example of an insider threat or adversary.

A list of the adversaries in Smart Grid environment that the National Institution of Standards and Technology – Smart Grid Working Croup introduces (NIST - SGWC) is described above in Table 2.1. The list is not complete but gives a good base to start from. In addition to this list, one might add, for example the press, the police, and national intelligence organisations.

Cyber warfare is currently a major and important part of military strategy for many countries [21]. Slowing and disrupting enemy forces without shooting a single shot is a great advantage. Moreover, gaining information on other countries' strategies and other sensitive information, can give a cutting edge, and create financial benefits. One example of an attack that might have been conducted by a nation-state is the Stuxnet worm that was discovered in July 2010. It was designed to target only specific supervisory control and data acquisition (SCADA) systems, possibly aiming to sabotage Iran´s nuclear program [22].

The press can be seen as some kinds of industrial spies, but with different motives and values; the public's right to know is the mantra used to justify many acts and publications [15, p. 50]. For example, in the United Kingdom (UK) a huge scandal was created when journalists were discovered phone-hacking people´s voice mails [23].

Depending on a country's state of welfare and level of corruption, the police forces may be considered as an adversary too. They do have the law on their side, but they are not below it. National intelligence organisations, like the Central Intelligence Agency (CIA), have more privileges than police forces, and for them, privacy violations, among other things, are everyday life. [15, pp. 43-58.]

According to Hyppönen [7], all attackers can be ultimately divided into three groups: online criminals, activist groups, and governments. The most obvious of these are the online criminals who aim to make profit by, for example, using a key logger to steal credit card numbers and so forth. The biggest of these online criminals are the multimillionaires whose locations are unknown. The activists, or "hactivists", attack because of an opinion, protest, or ideology, for instance. At the time of writing this thesis, probably the most famous activist group is Anonymous, who have conducted many successful attacks against different entities, such as Sony [24]. The third attack group is the most secretive, and also the most dangerous – the government. The motives behind their attacks vary from money to solving crimes. For example, according to Hyppönen, the attack against Dutch company DigiNotar that was a certificate authority (CA), could have been done by some government. What is more, it is plausible that people were killed in this attack.

2.4.3 Vulnerabilities

The main vulnerabilities that the attackers use are, among other things, backdoors, vulnerable devices, vulnerabilities in protocols and field devices, unpatched software and firmware, and improper security procedures. Unsecure wireless connections, databases, interconnectivity, and especially the users themselves [15, pp. 255-271; 25], can be, and should be treated as serious threats to an organization's information security.

Any modern automation system of today uses databases that are connected to a company's network. Structured Query Language (SQL) databases have gained a great deal of popularity but also have vulnerabilities that the adversaries try to utilize. For example, with an SQL injection or an XSS attack, it is possible to bypass the login, access sensitive data, modify content, or shut down the server, thus causing a lot of damage [20].

The lifespan of automation systems tends to be long, whereas the rotating cycles of, for example, operation systems are very short. Moreover, as the rotating cycle is short, and the programs are complex, daily updates are required to patch the security holes. This leads easily to a situation where the automation system software is not updated frequently, as the patches can break the sensitive system. [11, p. 90]

For most people viruses, Trojan horses, and worms are familiar at least on some level. These software, also known as malware, are categorized as malicious software. Malware most usually consists of a payload and a propagation mechanism, where the payload is the part that does the damage. This damage can be anything from displaying an annoying message to screen to modifying the access control permissions. The propagation mechanism is the part that spreads these malware; viruses live in other software and infect them, whereas worms live on their own, copying themselves to other computers. Trojan horse, on the other hand, is a piece of software that installs itself in one's machine to some software and hides there. [11, pp. 19-21; 15, pp. 151-152.]

The software of today are getting more and more complex, and thus making a 100 % secure software is virtually impossible. Security updates trying to patch the security

holes of faulty codes are more than common. In fact, most security problems are the result of faulty code. Attackers have used and will continue using these security flaws ruthlessly: buffer overflow means a flaw in the program that makes the program write data to an adjacent memory, out of the buffer's boundary. If this happens, the attacker might be able to access and modify the internal memory of the computer. These kinds of vulnerabilities are the most common ones and easiest to exploit. [11, p. 21; 15, pp 202-211.]

E-mail is part of everyday life for most people living in the occidental world. However, e-mail has no built-in security, but includes many security issues instead. Spamming has become the plague of today, covering more than half of all e-mail traffic. E-mails are also most often used as a propagation channel for malware and snooping of all kind of passwords. [11, p. 22; 15, p. 200.]

Unfortunately, there are also security gaps in network protocols that are the cornerstones of any communication. Attacks utilizing these gaps are called pharming, and they pose real threats. For example, under the domain name system (DNS) protocol, the local name server does not check where the answer for its queries comes from and ignores any additional replies. This enables hackers to replace the correct address with a false one, and act, for example, as a fake bank's sign-in page. [15, pp. 177-179; 26.]

2.5 Security measures

The key of any defence is defence-in-depth. It consists of various components, and how these components fit together. Ultimately, the overall safety is the product of these components. The components of the information security strategy are protection, detection, and reaction. These components work in tandem, meaning that if the system has strong protection, it does not need good detection and reaction mechanisms. On the other hand, without detection it does not matter how long the protection holds if the attack will never be noticed. Continuing the same philosophy, without reaction the detection is worthless. Making things more complicated, sometimes detection and reaction mechanisms are impossible to make. In these cases the protection mechanism just has to be strong enough. [15, pp. 272-282.]

There are many sources of attackers and many ways to attack, but there are also ways to defend. These countermeasures have evolved too, including improvements in network best practices, more focused policies, regulations and directives, technical solutions and so forth. These countermeasures and defend components, some of which are sturdier than others, are based on the following security methods and technologies.

2.5.1 Cryptography, identification and authentication

The heart of any security system is in cryptology, authentication, and identification. In order to understand just how the security is built on the Internet, one must understand cryptography, certificates, identification, and authentication. Protocols and methods like IPSec, Virtual Private Network (VPN), Pretty Good Privacy (PGP), Se-

cure/Multipurpose Internet Mail Extension (S/MIME), and many others are built from different types of encryption and digital signature algorithms [15, pp. 85-86].

Cryptography is not new, but an old way to protect messages from being read by unauthorized people. One of the most known cryptography strategies was used in the World War II, where USA used Navajo Indian language to encrypt the messages [27]. The idea of cryptography is to modify the original message so that outsiders cannot make out the real content. There are basically two types of algorithm methods used in cryptography: diffusion and confusion. In diffusion, the letters in the original message are shifted according to some algorithm, whereas in confusion method, the letters are replaced with symbols. The most sophisticated, state of art cryptography methods are using both confusion and diffusion methods. [28.]

The principle of cryptography is in the keys that encrypt and decrypt the messages. If both encryption and decryption are done with the same key, it is called symmetric-key cryptography. The problem with this is the key management as each distinct pair must share a different key, raising the number of required keys to very high numbers. There is also the problem of securely establishing the connection between parties. The most common symmetric algorithms are Data Encryption Standard (DES) and triple-DES, Rivest Cipher 4 (RC) and RC5, International Data Encryption Algorithm (IDEA), Blowfish, and Advanced Encryption Standard (AES). [15, pp. 86-90; 29]

In public-key cryptography, there are two different keys; a public key and a private key. As it is not possible to compute one key from another, one can publish the public key. A sender can now use this specific key to send encrypted messages to the one that published the key. Now only the receiver who has the private key can read the encrypted message. However, the problem of the public-key cryptography is the performance, and it is more common to use so called hybrid cryptography. [15, p. 95; 29]

The idea of the hybrid cryptography is that the sender encrypts the message with some random symmetric key. Then the sender encrypts this key with the receiver's public key, sending both the encrypted message and the encrypted key to the receiver. Now the receiver can first decrypt the random key with the private key, and then decrypt the real message. This is how encryption works in most of the protocols, such as PGP, S/MIME, TCP/IP, and many others. However, one problem remains, and that is the management of the keys. [15, p. 96; 29]

Cryptography only takes care of encrypting the message. The integrity and authentication of the message can be assured with digital signatures. This means that the message was created by a known sender and is not altered in the transit. This is done by using public and private keys just like in public-key cryptography. Now however, the sender encrypts the message with her private key, and the receiver decrypts the message with the sender's public key. As the private key is known only by the sender, it becomes the signature of the sender. [15, pp. 96-98; 29]

However, the problem here is that the receiver can only be sure that the message is encrypted with the sender's private key but not about who really used that key. Certificates try to solve this problem by binding an identity and a public key. The identity can

be many things, such as the name of a person or organization, serial code of the computer, and so forth. The certificates are issued to users by a CA, which can be, for example, a private company. The CAs have different levels of hierarchy. The whole system is called a public-key infrastructure (PKI). Certificates are used for network access authentication and are more secure than password-based authentication methods. [15, pp. 96-97; 15, pp. 229-234.]

2.5.2 Technical solutions and methods

In addition to using technical solutions like firewalls, companies also have to adopt secure policies and methods to fight against adversaries [11, pp. 72-76;]. These can include, for instance, the procedures of hardening the OSs or backup policy. The following paragraphs concentrate on introducing the most important technical solutions.

Firewalls and virus protection are probably the most well-known software amongst normal people to protect oneself against malware. These solutions with some alterations are also used in companies. Firewalls can be software or a machine that protects internal network by controlling network transmission based upon a set of rules. With host based firewalls, programs can also be controlled. Firewalls are the boundaries between public and private networks and a starting point for information security. However, they cannot provide good level of security by themselves. [11, pp. 80-81; 15, pp. 188-193.]

Demilitarized zone (DMZ) is a logical or physical sub-network that connects a company's public services to a larger, untrustworthy network, such as the Internet [11, pp. 79-80]. This way an external attacker, for instance, would only have access to equipment in the DMZ. It is a crucial component of an organization´s overall safety.

VPN is a secure connection over a public network to connect networks or mobile users to other networks. It uses different cryptographic protocols, most common being IPSec. [11, pp. 85-86; 15, pp. 193-194]

Intrusion detection system (IDS) is a system that monitors the network, looking for suspicious behaviour, and alerting of an attack. For example, Snort, developed by Sourcefire, is an open source network intrusion prevention and detection system (IDS/IPS) that logs the network traffic, analyzes the core of the packets, compares protocols, and monitors the use and scanning of ports [30]. The problems with IDSs however, are false alarms, which eat away the reliability and trust of the system. [11, pp. 80-81; 15, pp. 194-197.]

Burglar alarms and honey pots are kinds of IDSs; they give an alarm when an attacker goes to a certain place. Whereas with burglar alarm the sweet spots are specific things, in honey pot they can be entire computers or subnets masked to look inviting to attackers. [15, pp. 197-198.]

A vulnerability scanner goes through computer files trying to find their known vulnerabilities. For example, Nessus, developed by Tenable Network Security, is a very popular vulnerability scanning program that can detect vulnerabilities like misconfiguration, default passwords, denials of services, and so forth [31]. However, vulnerability scanners can neither find every vulnerability, nor measure the effect of their actions

when scanning. Web applications, especially, are problematic to scan, since they might have vulnerabilities not only in the platform and running environment, but also in code itself. Code is hard to test from outside and for this reason there are different tools to test them. Regardless of this, vulnerability scanners have their place in security measures. [15, pp. 198-200.]

2.6 Security testing techniques

There are several different methods to analyze the information security of the system. All these methods have their own characteristics and are best used in certain places. Automation environment often requires special attention, and it should always be considered thoroughly before using a certain method. The following techniques are the most used ones and will also be used in the testing part later on in this thesis.

Network scanning is used for identifying active hosts, open ports, Internet protocol (IP) addresses, services, and detecting devices of the network. There are two types of methods for acquisition of information: passive and active. In the passive one, the network is only being listened to, whereas in the active one, a large number of packets are sent. The conclusions are made based on the analysis of the data listened to. The passive method requires more time but is, on the other hand, virtually impossible to detect even with an IDS. [1, pp. 109-110; 14, pp. 114-116.]

Vulnerability scanning is used to find well-known vulnerabilities of the system, such as unsafe old program versions. This method is important especially in an industrial environment, where programs are old and not updated frequently. On the other hand, vulnerability scanning will only find risks, and sometimes these found vulnerabilities cannot be fixed with any reasonable amount of money. [1, pp. 111; 14, p. 117.]

Fuzz testing is often an automated or semi-automated testing method used to find security problems in software, especially in network protocols. It is a black-box testing model, meaning that there is no need to either know how the program works precisely or need for source code. In fuzz testing, invalid data is entered to inputs in order to find vulnerabilities that make the program behave in an unexpected manner. Fuzz testing may not always detect all possible vulnerabilities, and sometimes profound data-flow analysis is the only way to find specific vulnerabilities. With fuzz testing, it is possible to find mainly the simplest flaws in the program. However, those found vulnerabilities can be severe ones, and ones that most hackers would use. Fuzz testing gives a rash evaluation of the reliability of the program and implies what parts should be monitored closer. [1, pp. 108-109.]

In penetration testing the information security level of the system is analyzed by attacking against the system. There are a few different methods for performing a penetration test. In black-box testing, there is no need for earlier knowledge of the system, and thus it simulates the situation where the attacker does not know the system. In white-box testing, the attacker has full knowledge of the system, simulating the situation

where attack comes from inside or it is the case of an information leak. [1, pp. 112-113; 14, pp. 107-109.]

Source code analysis can sometimes be the only way to test the program. The idea is to find, either manually or automatically, coding flaws from the source code. This should really be a part of the coding process where it can be easily managed, and where found flaws can be easily repaired. [1, pp. 113-114.]

3 SMART GRID

This chapter aims at clarifying the complexity of Smart Grid, and introduces the TUT demonstration environment. Understanding the idea and, most of all, the structure and building blocks of Smart Grid is important in order to comprehend the risks in information security.

To help analyze and figure out the Smart Grid environment, the conceptual model based on the guidelines of the NIST/SGWC is introduced. This model is used with the TUT demonstration environment to figure out the domains and the players involved.

3.1 The landscape

In the future, energy generation and distribution will be more decentralized and utilizes localized renewable resources [14, pp. 1-18]. Even now, some farms or little remote islands are utilizing other kinds of energy sources, such as methane or hydrogen, to generate energy in an independent distribution system [32]. It has also become more and more popular amongst people to have a solar cell on the roof in order to reduce energy consumption by using solar power for, for instance, heating hot water. To bring up an example, in 2010, about six billion watts of solar panels were installed in Germany [33]. In near future, the excess electricity that the solar cell, for one, produces, can be sold to the grid company by using intelligent devices that communicate with grid companies over a network; in other words, via Smart Grid.

Smart Grid is the name for a new electric grid that will supersede the old grid in the future. This new grid modernizes the electricity delivering system by introducing more intelligent devices, and information networks. Thus, it monitors, protects, and automatically optimizes the operations of the grid. Smart Grid will be international by default, and it thus, also creates international energy trading markets. This will surely have an impact on the price of electricity. According to the study made under work package seven in sub task two of the SGEM project, almost in every scenario used the price of energy will first rise, but after year 2030 it starts to decrease [34]. Altogether, Smart Grid will update the old electric grid, providing new functionalities, and improving the quality, availability, efficiency, capability of self-healing and dynamic of the grid. [35, pp. 6-7.]

The current deployment status of the Smart Grid is that it is in development. The process will take time, as the update is rather profound and vast. The transition will be gradual, taking one step at time. However, first steps are being taken all over the world towards Smart Grid [14, pp. 14-15]. Installation of smart meters to households has begun all over Europe with timeframes varying from the end of 2011 to 2015 [36]. South

Korea has announced that their goal is to have a fully integrated Smart Grid by 2030, which, if completed, would be the first one [37].

3.2 Infrastructure and architecture

Smart Grid will be a complex, integrated system consisting of sub systems. One way to divide Smart Grid is to think of it as consisting of layers. In the bottom, heart of the Smart Grid, is the power system layer, which takes care of the generation and distribution of energy. Above power layer is control layer that consists of sensors, SCADA systems and such, to help control the power system. These two layers are also in the current electric grid. However, Smart Grid also utilizes an ICT system, which consists of communication, IT, and application layers. Somewhere between communication and IT layers there is also the information security layer. [38.] In the scope of this thesis, the ICT side of Smart Grid is more relevant, and thus the concentration is there as well. The high-level overview with the power and ICT systems of the Smart Grid is presented below in Figure 3.1. This figure is also presented in appendix B.

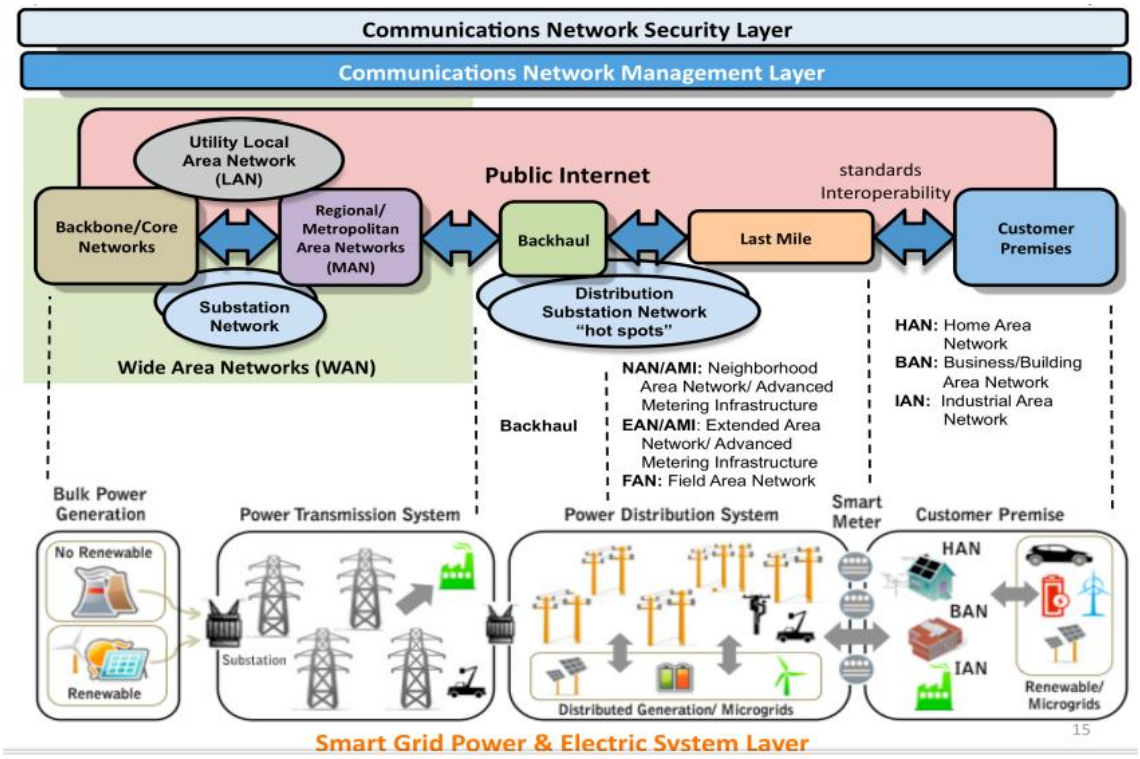

Figure 3.1. *High level picture of communication and power layers [38].*

The power system consists of power plants, transmission lines, substations, and end users. Power generation facilities are, for example, wind turbines, nuclear power plants, water turbines, etc. Electricity is transmitted via transmission lines from one point to another. Before the end user can use the electricity, the voltage level is lowered in transmission substations and distribution substations. The end user can be industrial, commercial or residential. The produced voltage level depends on the type of end user. The power system also includes networks, such as the power control network, that are used to operate and monitor the electric grid. [35.]

The cornerstones of the information system are the communication networks above which security and application layers are provided. The communication networks consist of sub networks, zones, providing means for devices to communicate. The zone in a customer's premises is called Home Area Network (HAN), or sometimes also referred to as Premise Area Network (PAN), or Building Area Network (BAN). This zone includes devices communicating over one or more networks. Field Area Network (FAN) is a zone that includes devices communicating between the individual service connections and backhaul points leading to the utility. It also includes distribution automation and control devices. The backhaul is a portion of the network that comprises of the intermediate links between the core network, and the small sub networks. Advanced Metering Infrastructure (AMI) supports this zone. Substation Area Network (SAN) zone includes devices, such as capacitor banks and relays, communicating inside a single electric substation. The zone bridging the FAN and SAN, the utility Local Area Networks (LAN), and the back office is called Wide Area Networks (WAN). It also includes communications from control centres to the substations. [39, pp. 9-10.]

The profound innovation of Smart Grid is the new decentralized architecture. As shown in Figure 3.2, current electric grid uses centralized architecture, where electricity flows one way only from bulk generators to end users. Decentralized architecture, however, enables energy generation in a more flexible manner, as there is no straight, tree-like architecture; there are multiple routes to nodes so that smaller areas can be isolated in case of disturbances. Also, decentralized architecture enables local distribution and consumption of energy, thus enhancing the efficiency of the grid. This will be possible due to the two-way flow of electricity and information, and the distribution of intelligence on the lower levels. Altogether, the architecture of Smart Grid will bring flexibility, and in some way carries great resemblance to the architecture of the Internet. [40.]

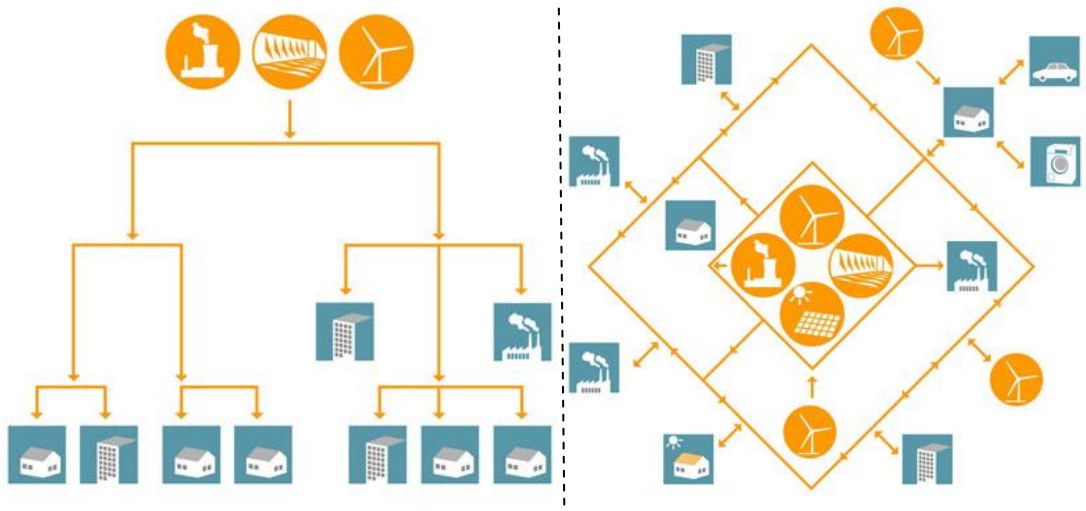

Figure 3.2. *The architecture of the old electric grid and the new Smart Grid [40].*

Smart Grid is really a network of networks. It brings together different networks by utilizing public networks, such as the Internet. The nationwide network, for instance, consists of smaller networks, which are interacting with each other. These smaller networks can be, for example, municipality networks consisting of even more sub networks. The high level view of the information network for the Smart Grid is shown in Figure 3.3.

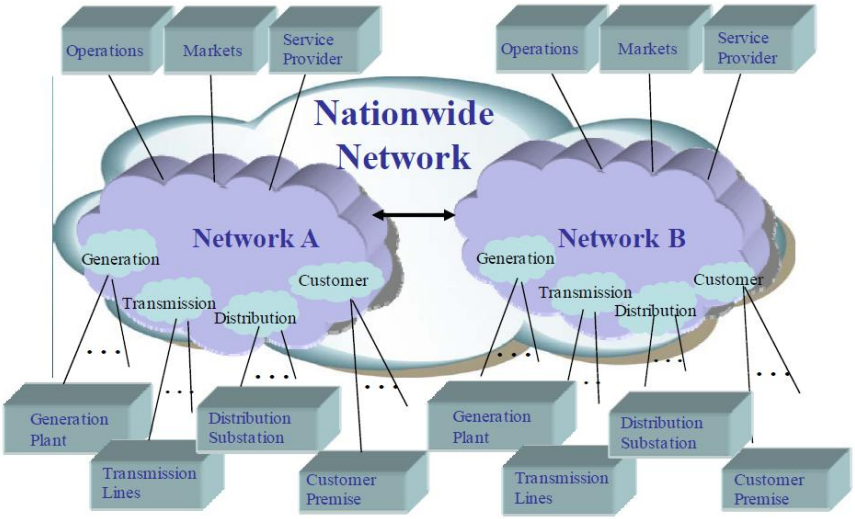

Figure 3.3. *The information network of the Smart Grid [35, pp. 16-18].*

Same principle goes for international networks. This way, Smart Grid enables interaction between national grids, and offers an efficient way to import and export electricity on many levels.

3.3 Benefits

There are great many benefits in Smart Grid, some being technical, some economical, and some even environmental. There is also a countless number of other benefits, some being hard to discover beforehand, such as changes in attitudes towards energy consumption.

From an environmental point of view, the most important benefit is that Smart Grid encourages the use of renewable energy sources, such as solar cells. Current status in most of the well-fare countries is that customer cannot sell electricity that is self generated by using, for example, solar cells to the grid. With Smart Grid it will be possible to sell, and profit economically from these kinds of energy sources. This enhances the use of renewable energy resources, and is thus an important way to reduce emissions and global warming [35, pp. 6-9; 40]. Moreover, there might be a change in people's attitudes towards the consumption of energy, as it becomes a part of their everyday life, and forms into a more concrete way to really affect their economics.

From an economical point of view, the most important benefit of Smart Grid is the enhanced efficiency [35, pp. 6-7]. There have been many calculations and estimations of how much Smart Grid will, in the end, save money. In Europe, according to a study made in last fall, Smart Grid could save as much as 52 billion Euros per year [41]. Also, it is not said how many new jobs will be created, and how many new companies founded. On the other hand, building a Smart Grid is not free; it requires a lot of resources and money. Nevertheless, in the long run, it will be more than profitable.

The technical point of view, which enables the other points of view, includes many important benefits. Maybe the most important one is the improved efficiency of the grid: household equipment, such as fridges and electric vehicles, can be used as a means to minimize excess power generation. Moreover, current electric grids around the world are several decades old, and thus not working as efficiently as they used to: transmission and distribution losses are ever growing numbers. Smart Grid also adds intelligence to the grid enabling local distribution and consumption of energy. The capability of self-healing makes it more reliable, and more efficient. [35, pp. 6-9; 40.]

3.4 Players

The players of Smart Grid include a broad spectrum of different stakeholders having different roles and responsibilities. In many ways, Smart Grid resembles Internet. These players can be classified into five different sub-groups: grid operators, grid users, energy market place, providers of technologies, products and services, and influencers [42; 43]. The figure describing the most significant players of Smart Grid is presented in appendix B.

The electric grid can be split into two major subsections; the transmission and the distribution networks. The transmission networks are the backbone of the grids, and operated by transmission system operators (TSO) or independent systems operators

(ISOs). TSO is a non-commercial organization – usually at least partly owned by the state or government – responsible for an area to be electrically stable, and for the security of supply in this area. The TSOs of the Nordic countries, for example, are Statnett SF (Norway), Svenska Krafnät (Sweden), Fingrid (Finland) and Energinet.dk (Denmark).[44; 45]

The distribution systems are operated by distribution system operators (DSO), and their purpose is to distribute power from the transmission network to customers. DSO is quite like TSO, and responsible for regional grid access and grid stability, integration of renewable energy sources at the distribution level, and regional load balancing. For example, the three biggest DSOs in the Nordic countries are Fortum, Vattenfall and E.ON. [44; 45]

Both TSO and DSO have neutral monopolies to avoid unnecessary duplication of infrastructure, and to guarantee access to all players at equal conditions. A neutral monopoly means a situation, where the most economically efficient state is gained by only one supplier. Distributor might also act as a supplier, but is obligated to distribute power from any other supplier under the same terms.

Grid users can be divided into electricity producers, suppliers, and consumers. Energy producing companies have traditionally been operating mostly large power plants connected to the transmission network. Now, however, also small producers, such as small wind farms, connected at sub-transmission and distribution levels with very different characteristics are supplemented. [42.] The three major players in Nordic production markets are Fortum in Finland, Vattenfall in Sweden and Statkraft in Norway [45].

Consumers will become more engaged in Demand Side Response (DSR), which means that consumers will response more fiercely to high prices of electricity. Consumers can make more informed decisions on saving energy either by changing their behaviour, or by engaging with an energy efficiency service provider. [42.]

Suppliers buy power either directly from a producer or through the energy exchange, and resell it to companies and households. To make DSR possible, suppliers will have to use dynamic load profiles, and complement this information with the actual information about market activities of consumers, producers and those who act on both sides, to the DSOs/TSOs. The supplier has a grid connection and access contract with the TSO or DSO, providing new services, real-time information, energy efficiency services, and dynamic energy pricing concepts with Time-of-Use. In Nordic countries, for instance, the three following suppliers stand for a quarter of the supply: Fortum, Vattenfall and Dong Energy. [42; 45.]

The energy production can be traded through bilateral contracts between suppliers, retailers, and end customers, or through a power exchange market place. Clearing and settlement agent acts as a contractual counterparty within a power exchange market, and for bilateral contracts. It assumes liability for covering the future settlement of these contracts. A trader is a player who owns the power during the trading process, buys or sells energy and services in power exchange market or bilaterally. A broker, on the

other hand, does not own the power but merely acts as an intermediary. To mention an example, Nord Pool Spot is the leading physical power market in Europe. [42; 45; 46.]

A significant group of players in Smart Grid are the companies providing technologies, products, and services to the grid. This group consists of a vast variety of different companies providing different state-of-the-art technologies and solutions, for instance, metering operators and building energy management systems. [42.] One major player in this section is ABB.

The influencers of Smart Grid can be divided into grid users, regulators, standardization bodies, and EU and national legislation authorities. Grid users and how they perceive the value received from other actors have a great deal of influence on the economic viability of the grid. Regulatory authorities ensure that companies under regulatory laws remain economically efficient, and both generation and retail companies adopt fair and transparent practices to the benefit of the customers. In Finland, for example, the regulatory authority evaluates the reasonableness of capital expenditure by means of a standard cost catalogue in which Smart Grid investments are treated like any other investment. Be the Smart Grid components more expensive than normal ones, then companies have to negotiate higher price. The regulatory authority then decides whether to promote these kinds of investments. [47, p. 19.] Standardization bodies are responsible for standardization of all components within the supply chain, whereas EU and national legislation authorities are in charge of defining legislation and policies such as environmental policy, and so forth. [42; 43.]

3.5 The conceptual model

NIST, a federal agency of the United States Department of Commerce, introduces a conceptual model of Smart Grid. The purpose of the conceptual model is to deepen the understanding of the building blocks of an end-to-end Smart Grid system, and demonstrate how these blocks interact with each other. The conceptual model provides a high-level framework for Smart Grid that defines seven domains*: Bulk Generation, Transmission, Distribution, Customer, Operations, Markets* and *Service Provider.* Each domain consists of Smart Grid elements – *applications* and *actors* – that are connected to each other through two-way communications and energy paths – *associations* – through *interfaces*. The conceptual model shows all the communications and energy flows related to each domain, and how they are interrelated. [13, p 15; 35, pp 21-22; 48.] Figure 3.4 presents the domains of the Smart Grid, and the electric and information flows.

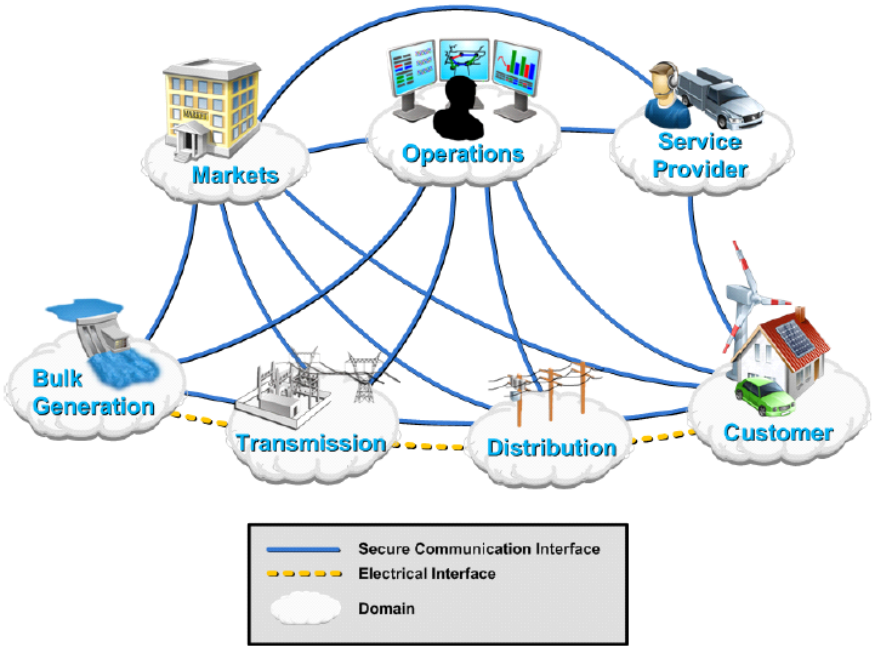

Figure 3.4. *The top-level view of conceptual model of Smart Grid [35, p 22].*

As can be seen, the electricity generation and distribution chain is provided in the bottom domains, those being bulk generation, transmission, distribution and customer domains. Information, on the other hand, flows in every domain.

3.5.1 Domains and actors

A Smart Grid *domain* is a high-level grouping of organizations, buildings, individuals, systems, devices, or other *actors* with similar objectives, and relying on — or participating in — similar types of applications. *Domains* have overlapping functionality, and are not organizations. For example, a distribution utility also has actors in Customer domain, such as meters. All seven domains are described below in more detail. [13, pp. 14-15; 35, p. 22.]

The *Bulk Generation* domain generates electricity in bulk quantities, and may also store energy for later distribution. The sources can be anything from renewable sources like solar and wind, to non-renewable sources like coal and gas. The Bulk Generation domain is electrically connected to the Transmission domain, and has interfaces with the Operations, Markets, and Transmission domains. [35, pp. 34-36; 48.]

The *Distribution* domain distributes the electricity to and from *Customers*. It is the electrical interconnection between the Transmission domain, the Customer domain and the metering points for consumption, distributed storage, and distributed generation. It uses a two-way wireless or wired communication network to connect the smart meters and all field devices, managing and controlling them. Energy storage facilities, and alternative distributed energy sources may also be connected to the *Distribution* domain. The Distribution domain communicates closely with the Operations domain in real-time

to manage the power flows associated with a more dynamic Markets domain. [35, pp. 38-39; 48.]

The *Transmission* domain transfers the bulk of electricity from generation sources to distribution through multiple substations. It is typically operated by a Regional Transmission Operator or Independent System Operator (RTO/ISO), who maintains stability of the grid by balancing supply and demand in transmission network. The Transmission domain may also contain Distributed Energy Resources, such as electrical storage. To control and monitor the transmission network, typically a SCADA system is used. [35, pp. 37-38.]

The *Customer* domain connects the end users of electricity and the electric distribution network through the smart meters, which provide information about customer's energy usage and patterns. Traditionally, there are three kinds of customer types, each with its own sub-domain and two-way communication networks: residential, commercial/building, and industrial. The energy needs for each sub-domain are typically set at 20 kW for residential, 20-200 kW for commercial/building, and over 200 kW for industrial. The Customer domain is connected electrically to the Distribution domain, and communicates with the Operations, Markets, Service Provider and Distribution domains. The boundaries of the Customer domains are typically the utility meter, and the Energy Service Interface (ESI). ESI is the primary service interface to the Customer domains, and it communicates with other domains via the AMI infrastructure, or via, for example, the Internet. The ESI communicates with devices and systems within the customer premises using a LAN. The ESI provides a secure interface for Utility-to-Consumer interactions, and can act as a bridge to facility-based systems such as the customer's energy management system (EMS). The EMS is the entry point for such applications as, for instance, remote load control, monitoring, and control of distributed generation. [35, pp. 26-27; 48.]

The *Operations* domain manages and controls the electricity flow of all other domains. It uses a two-way communications network, and provides monitoring, reporting, controlling, supervision, and process information. EMSs are used in transmission operations to analyze and operate the transmission power system reliability and efficiency, while Distribution Management Systems (DMS) are used in distribution operations for similar purposes. [35, pp. 31-34; 48.]

The *Markets* domain operates and coordinates all the participants in electricity markets by providing market management, wholesaling, retailing, and trading of energy services. It interacts with all other domains and handles energy information clearinghouse operations and information exchange with third-party *service providers*, for example, roaming billing information for inter-utility plug-in-vehicles. The communication between the Market domain, and the domains supplying energy – Bulk Generation domain and Distributed Energy Resources (DER) – is critical, for the production and consumption is dependent on markets. DERs may be located in Transmission, Distribution, and Customer domains and are typically served though aggregators. The bounda-

ries of Market domain are at the edge of the Operations domain, the domains supplying assets, and the Customer domain. [35, pp. 28-29; 48.]

The *Service Provider* domain includes all third-party services to support the business processes of power system procedures, distribution, and customers, for instance, web portals that provide energy efficiency management services to end-customers, or outage management for the utilities. The Service Provider domain has interfaces with the Market, Operations and Customer domains. The communications with these domains are critical for system control and situation awareness, and for enabling economic growth. [35, pp. 29-31; 48.]

The following figure represents the domains of Smart Grid more precisely with the most important actors and interfaces. This figure is also presented in appendix B.

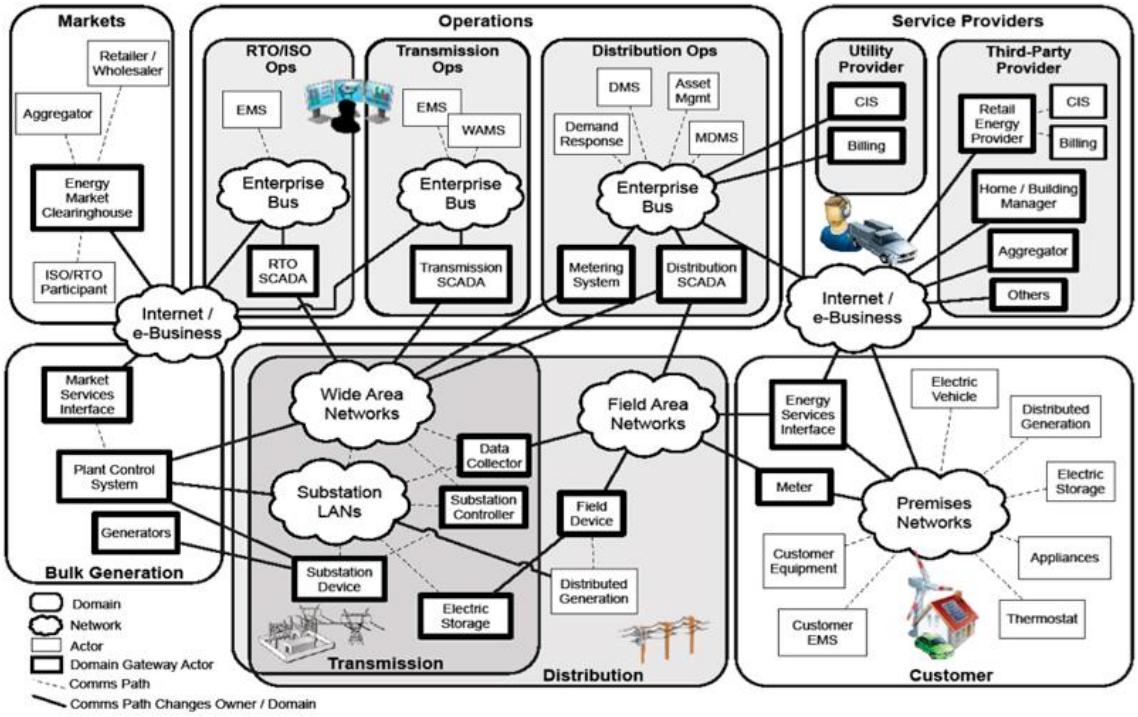

Figure 3.5. *The top-level view of conceptual model of Smart Grid [49, p. 35].*

Actors are devices, systems, programs or individual organizations that participate in the Smart Grid, such as smart meters. They exchange information with other associated actors through *interfaces*, and have the capability to make decisions. An organization may have actors in several domains. *Applications* are performed within a domain by one or more actors; for example, solar energy generation and energy storage, and energy management. *Associations* are logical connections between actors that establish bilateral relationships, and *Interfaces* represent the point of access between domains. [35, pp 22-23]

3.5.2 Differences between North America and Europe

North America is the pioneer of the Smart Grid, and is the reference model to Europe in the deployment of Smart Grid. By studying North America's process, Europe can avoid some pioneer mistakes made in the U.S. Since we are using the U.S as reference, it is also vital to understand the differences between these two environments. These differences can be grouped under three categories: technological, operational, and policy.

In North America, the American National Standards Institute (ANSI) is responsible for managing metering standards, whereas in Europe this is managed by the International Electrotechnical Commission (IEC), and Measuring Instrument Directive (MID). This creates requirements for different products in the Europe and in the U.S. On both continents, the Smart Grid systems use a TCP/IP based communication, but with different meter communication protocols. The European meters are using DLMS/COSEM suite of standards, whereas in the U.S, they are using NASI C12.18 and C12.22 communications. This results in differences in head-end software, and low-level communication components. Additionally, in U.S, the Smart Grid is using mesh technology, whereas in Europe power line communication (PLC) and digital cellular communications are utilized. However, the recent developments in wireless mesh technologies indicate that it will be taken into use in Europe too. Even though the radio emission standards differ, the architecture will be similar in the U.S and in the Europe. [50.]

There is also difference in the operation management between the two continents. The meters used in Europe are roughly estimated half the price of the meters used in the U.S. In addition to this, the use of air conditioners is substantially larger in the U.S, which affects the peak demand. This makes the operational business benefits much larger in North America [50]. On the other hand, the cheaper meters used in Europe may not be so cheap after all, as they are not so reliable. For example, a Finnish DSO company had to change 22 000 meters because of a bad component [51]. It must also be taken into account that Europe has many cultures, which might make it more difficult to predict user behaviour causing peak demands, like baking the Christmas ham, or heating up Saunas at weekends.

In Europe, each country has the individual authority of implementation of Smart Grid. However, they follow the guidelines of Smart Grids European Technology Platform for Electricity Networks of the Future, a centralized mandate. In the U.S, there are no national, centralized mandates; thus, certain states are moving faster than others. Unlike the U.S, Europe has listed Smart Grid to their plan against global warming, which is catalyzing the process. Europe is ahead of North America in the use of renewable energy sources, and will profit more from the Smart Grid. [50; 52.] There are also differences in legislation and privacy policies. In the United States, people do not own their own data, and most privacy violations are legal, such as, for instance, data collecting. In the EU, however, privacy policies are much more restrictive. [15, p. 29]

3.6 Smart Grid demonstration environment

As a part of CLEEN's SGEM project, the department of electrical energy engineering of TUT made a laboratory demonstration environment for Smart Grid applications in the year 2011. It includes both the information and the automation systems, as well as the active resources. The ICT system of the laboratory environment consists of distribution network opetator control centre software, aggregator, home energy management system (HEMS), and interfaces between these. There is also a group of active resources available. Figure 3.6 below describes a general top-level view of demonstration environment, and how the equipments are connected to other utilities.

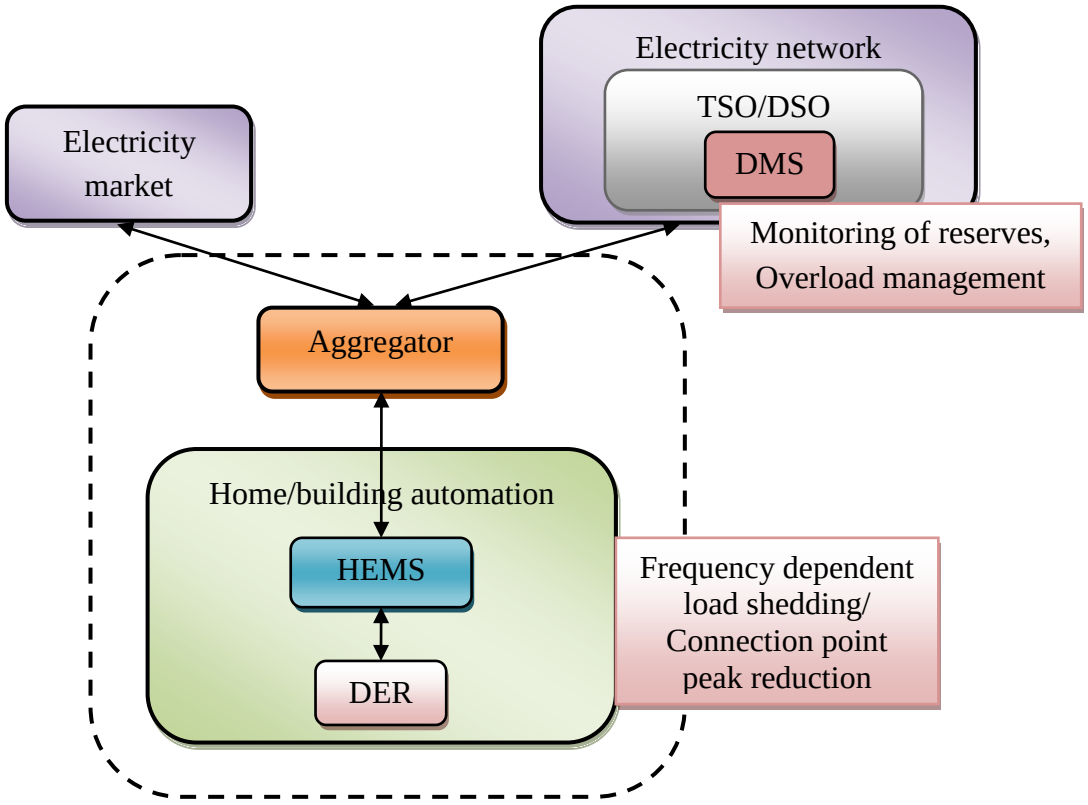

Figure 3.6. *The Smart Grid demonstration environment.*

HEMS manages DERs – small-scale resources – by collecting measurements and making decisions, also providing an interface to these resources. Small-scale resources are resources that are typically owned by the end costumer, such as hot water boilers, electric vehicles and so forth. HEMS includes both ESI, and customer's ESM. In order to keep the processes and decision making fast enough, aggregation of information is required. An *aggregator* is a centralized information integrator quite like SCADA that collects, stores and aggregates information from, for example, HEMS. It provides relevant information such as operational information, contract details, billing information

and parameters of active resource controllers, and applications to higher level decision-makers, such as Industrial Control System (ICS). [53, pp. 8-9.]

3.6.1 Use cases

Use case is a description of how actors work together to reach a goal [35, pp. 24]. There is a countless number of possible use cases related to this ICT and electricity distribution network automation system. The following paragraphs describe two possible use cases that utilize this environment.

Monitoring of reserves

As described above, a power system requires controllable loads to balance system frequency and voltage in normal and disturbance situations. The large-scale resources have to be monitored in real-time, but in small-scale resources this would require enormous investments on the ICT system. However, real-time monitoring of reserves is not required, since the capacity of resources can be statistically forecasted. Many automatic reserves can also be operated based on local measurements, and real-time communication to TSO control centre is not needed. However, monitoring of these reserves is needed, for the system must not compromise the reliability of the power system. [53, pp. 10-11.]

In order to smoothen and improve the monitoring of reserves, hierarchical levels – increasing delays towards the small-scale resources – and classification of resources – normal/disturbance, response time and capacity – should be introduced. This way non-real-time monitoring, short- and long-term statistical forecasts of resources, and the knowledge of what kind of reserves are available is gained. [53, p. 11.]

Network overload management

With Smart Grid, it is possible to supervise in real-time the overload of the network, and thus increase the network utilization rate. Centralized network overload management is based on the comparison of results to maximum loading values, and real-time measurements, load flow calculations, or state estimation of managed network. [53, pp. 13.]

Overload management is a control centre function implemented, for example, to the DMS, which gets real-time measurements via the ICT system. Based on the information that the DMS receives, it calculates the best possible estimate for network voltages and currents. The analysis of network overloading can be distributed to lower levels, and much closer to measurement point and control resources. [53, pp. 13.] The domains, actors and players

3.6.2 The domains, actors and players

The analysis introduced here is made based on the guidelines of NIST/SGWC. The starting point of the analysis is identifying related use cases, and dividing the demon-

stration into *domains* and *actors*. After this it is easier to comprehend relevant interfaces and vulnerabilities.

The domains of the use cases introduced earlier include Customer, Service Provider, Operations, Transmission and Distribution. Markets domain can also be very relevant in similar environment but with different use cases. In customer domain, the actors are ESI, EMS, and devices. The HEM system includes both ESI and EMS actors. In service provider domain, there is only one actor, the aggregator. The operations domain has SCADAs, DMS and EMS actors. The distribution and transmission domains do not have actors.

The situation described here includes a range of different players that are, one way or another, involved in it. Starting from the equipment, there are the manufacturers of the HEM system, aggregator, SCADA, DMS, EMS and home devices. The users and owners of these equipment are most usually a different entity or person than the one that developed them. For example, the HEM system may belong to the customer or to the Internet Service Provider (ISP); the aggregator may belong to some Service Provider or to DSO; SCADA, EMS and DMS are operated by TSOs and DSOs; the home devices are used by the customer. Then there are the players who provide services, such as the TSOs and DSOs, ISPs, aggregators and so forth. These players also operate over the domains, for example, the DSO operates mainly in Distribution domain, but also in customer domain with the smart meter that it owns. This is the general situation, the one that the laboratory demonstration is simulating. Figure 3.7 below presents which domains and actors are involved, and how these are connected to each other.

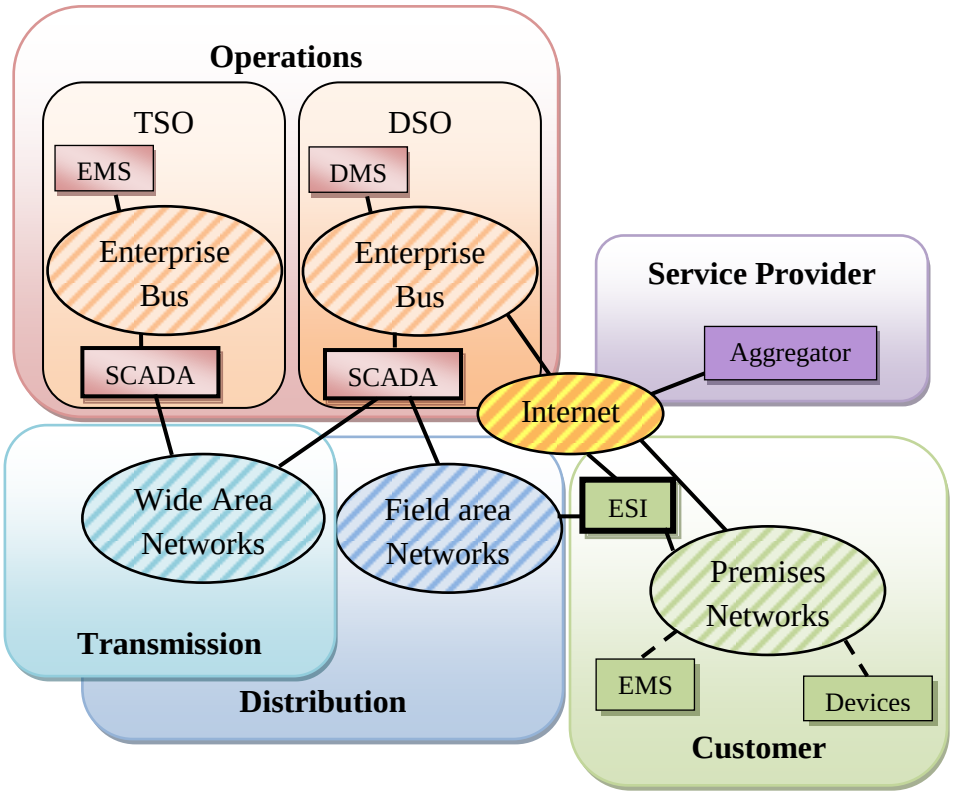

Figure 3.7. *The domains, actors and networks of simulated environment.*

In the figure, different colours represent different domains, for example, green is a colour of customer domain. The striped ellipse areas represent networks, whereas the rectangular areas represent actors. The domains are presented with rounded rectangles.

The actual demonstration testing environment is simpler than the one it is simulating. For example, in the laboratory environment everything is run in TUT´s Intranet, instead of using ISPs public networks [53]. Additionally, the roles of the electricity transmission and distribution, as well as most of the customer roles are left to the background in the demonstration. The *players* of the laboratory demonstration environment are: ABB in Operations domain, NSN in Service Provider domain, There in Customer domain, TUT in Service Provider, and customer in Customer domain. These equipment are managed in demonstration environment by TUT staff. Figure 3.8 below describes the overall situation of the laboratory demonstration environment with domains, actors, networks and players involved.

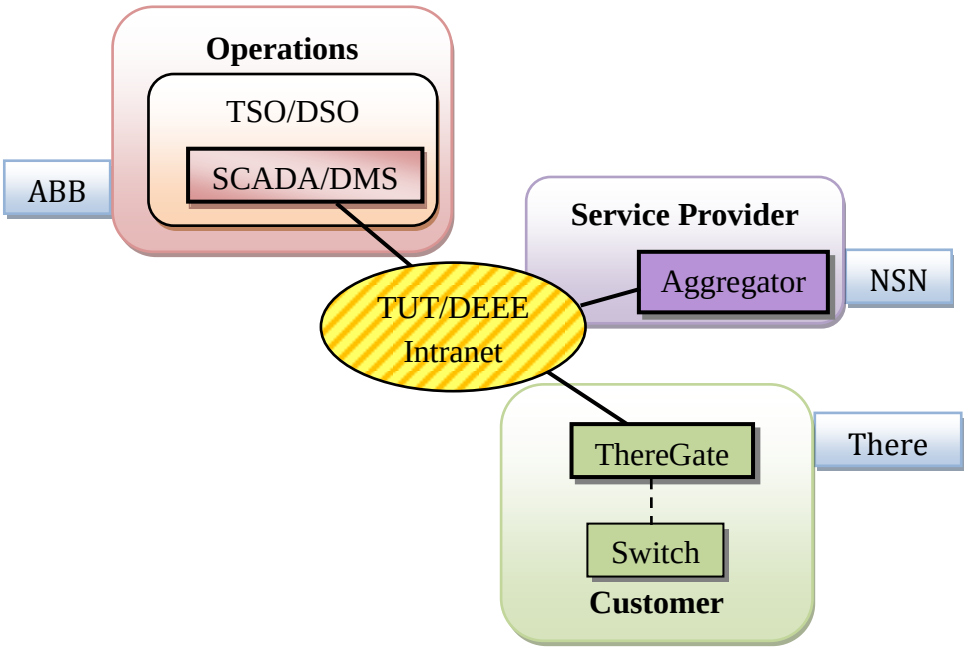

Figure 3.8. *The domains, players, equipment, interfaces and players of the demonstration environment (See Figure 3.7, the colourcodes are equivalent).*

As Smart Grid is a system of systems and has a variety of players, there is no mutual goal that would satisfy everyone. One example of this kind of situation is from the study made in Massachusetts Institute of Technology (MIT). The study indicates that real-time information about the price of energy may result in a huge demand spike, if too many people follow the fluctuations, and turn on devices when the price of electricity crosses the threshold. This could, in the worst case, bring down the entire power grid. Fortunately, this can be prevented by simple types of price control. These price controls, however, reduce the efficiencies that the real-time pricing would bring. A more costly, but, in the end, a more efficient solution would be modelling the end users to respond to

different prices at different times. [54.] However, one thing that is common for all these stakeholders is that if the Smart Grid does not work, it will affect all. Thus, assuring that the Smart Grid will work in every condition is a common business advantage for all. One major part of securing Smart Grid is information security. In other words, information security should be one of the most important things in every stakeholder's politics.

Being a complex environment, these players cannot, in most cases, act alone, but interact with other players. These interactions between players can be places of vulnerability, and require special attention. Usually, the information security of these interconnections is a matter of agreement between the companies involved, which, in the end, is a matter of trust.

3.6.3 Laboratory demonstration equipment

At the time this thesis was written, the home devices supported include thermometer and humidity sensor, motion detector, switches that include energy monitoring, and electricity meters either on Z-Wave or M-Bus. The first application made to this demonstration environment is frequency dependent load shedding. The idea of the demonstration environment is that it would be applicable for multiple Smart Grid applications. [53.]

The equipment on the top level of the hierarchy in the demonstrations environment is the ICS, which is used to supervise, monitor, and control the system. The ICS of the demonstration consists of MicroSCADA Pro SYS 600 and MicroSCADA Pro DMS 600, both developed by ABB. [53.]

The heart of the aggregator, developed by Nokia Siemens Network (NSN), is an element management system called Open EMS Suite (OES), which is a software platform for developing operation support system solutions. The aggregator also includes mediation components in order to communicate with lower-, and higher-layer network elements. Mediation is a software component that performs the necessary data conversions and protocol-level integrations between systems. [53; 55.]

The mediation between OES and ThereGate is called Agent. It runs on some computer, other than OES, and is connected via the Internet to both OES and ThereGate. For each ThereGate, there is one Agent. The idea behind this structure is that, later on in real environment, hundreds of Agents could be accommodated in separate computers in the LV network. The mediation between OES and SCADA is called Northbound Mediator. It runs on some computer similar to Agent, and has Internet connections with both OES server and SCADA server. [53.]

The HEMS of the demonstration environment is called ThereGate, developed by There Corporation. It is basically an advanced wireless router that runs on OpenWRT, open source Linux platform being a technology independent platform. Currently Z-Wave and WLAN are the only supported wireless technologies, but other technologies, such as GSM/GPRS/3G and ZigBee, will also be integrated in the future. With additional USB adapter, M-Bus can be integrated. [53; 56.]

4 APPLIED THREAT MODELING

This chapter presents the concept of threat modeling, and applies it to the TUT Smart Grid environment. The idea of this threat model is to provide a more general level perspective of the environment, as in the later chapters a more detailed analysis will be provided.

Threat modeling is a technique that helps to think about the security threats the system might face. Nowadays, threat modeling starts from a planning process, where threats are identified, and suitable countermeasures taken into account. This way, the attitudes towards information secure coding are increased. Nevertheless, computer programs of today tend to be somewhat complex, which makes creating 100 % secure applications virtually impossible. The basic idea behind threat modeling is the idea that every system has something worth protecting. These are called assets. The system, however, has vulnerabilities that attackers are trying to use in order to access the assets. These create threats and vulnerabilities in the system. The security countermeasures try to mitigate these threats, and prevent damages. [14, pp. 153-154; 57.]

4.1 The scope and limitations

According to SGIP/CSWG, customers can be divided into three different types: residential, commercial, and industrial [49, p. 32]. These three users have a great deal of differences: the network structure, the type of adversaries, the type of attacks, the assets and so forth. Each case must be treated separately, identifying the special need of that environment. For example, a commercial customer, such as a shopping mall, wants to offer wireless local area network (WLAN) Internet services to the customers, or services such as charging one´s electric vehicle in the future. Same services may be provided in the private costumer´s premises, but the environment is rather different, which creates different security issues. In addition to this, the consequences of a possible penetration can vary depending on the customer: for example, a successful attack in an industrial environment has potential to cause devastating damage to the entire society, whereas in private households the-worst-case-scenarios are not that grave.

The threat model of this thesis is derived from SANS Threat Modeling principles, keeping in mind the Smart Grid environment [57]. The domains that this environment includes are Customer, Service Provider, Distributor, and Transmission domains. However, this threat model is made from the end users perspective, and focuses on the Customer domain, especially HEMS.

4.2 Viewing the system as an adversary

Stepping into the shoes of the adversary gives valuable information on how the attacks could happen, and which vulnerabilities they might be utilizing. Studying the system from the outside, from the point of view of the adversary, and identify all entry and exit points of the system is the first step. Thinking like the adversary also helps to figure what are the assets of the system. [57; 58.]

4.2.1 Entry and exit points

In order for the components to interact and exchange data, there must be interfaces, entry and exit points that these components use. SGIP/SMWG introduces a logical reference model of Smart Grid, which contains seven *domains* and *actors* with *interfaces* between them. This model was used to find the actors and interfaces of the system. The model is presented in appendix C. From the TUT environment, the following actors were found:

- SCADA
- Aggregator
- Customer EMS
- Meter
- Distributed energy resources
- Customer appliances and equipment
- Electric vehicle
- Premise display

The actors, domains, and interfaces between these actors are presented in Figure 4.1. Distributed energy sources, premise display, customer appliances and equipment, and electric vehicle actors are in the same box since their logical interfaces are the same.

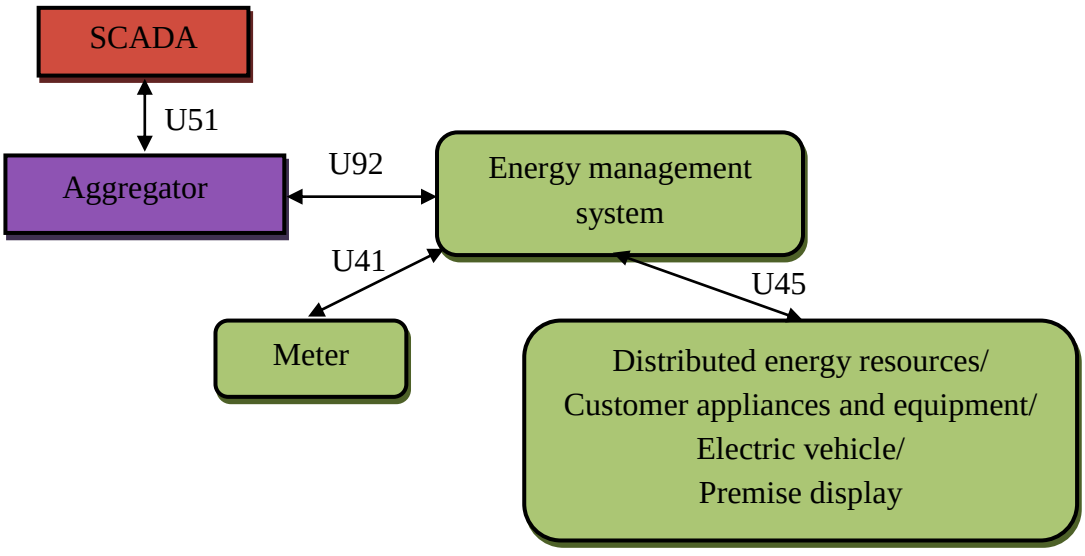

Figure 4.1. *The actors and interfaces of monitoring of reserves.*

Table 4.1. *The identifications, names and descriptions of the demonstration's entry and exit points.*

Logical interface category	ID	Name	Description
16th	U1	AGG-HEMS	Interface between aggregator and HEMS. HEMS provide information about local resources and such to aggregator.
18th	U2	HEMS-METER	Interface between HEMS and meter. Meter provides metering information about for example electricity.
15th	U3	HEMS-UI	UI to HEMS for end user. HEMS provide UI where user can monitor and manage HEMS, devices and resources.

There are more interfaces inside the system, for example, inside an aggregator or ICS, than the figure presents. However, as these interfaces are inside actors, they are not the first ones to be attack against. Despite that, certain amount of attention must be applied to these interfaces too, for if the attacker is able to penetrate the "first wall", there must be other "walls" to protect the system too.

Three of these interfaces are relevant from the end users point of view. The interfaces can be divided into logical interface categories according to the SGIP/SMWG division [13, pp 26-71]. These logical interfaces are presented in appendix C. The above Table 4.1 describes the logical interface categories, identifications, names, and descriptions of the interfaces.

Between HEMS and aggregator, a great deal of information about customers is transferred and handled. Some of this information is rather sensitive, and should be treated as confidential and private to prevent unauthorized access to it. Also, a great many interactions and appliances are taking place, meaning that if the data is invalid or wrong, it will have a large impact. However, most interactions are neither real-time based, nor have any connection with the power system operations.

The location of HEMS will be at the customer´s premises. This means that the physical safety of ThereGate is left, at least partly, to the responsibility of the customer. Keeping in mind that ThereGate will be implemented to every household, it is certain that some of these people are criminals, and possible adversaries to Smart Grid. For example, it might become a luring idea to try manipulating one´s energy consumption information in order to gain financial profit from it. In order to maintain at least some level of physical safety of ThereGate, seals or other solutions need to be applied. However, it is only a matter of time when someone figures out a way to bypass the seal, and puts the information to the Internet for everybody to see. In the end, there is no way to prevent the crime for happening, but there are ways for knowing and proving that it has happened. HEMS can also be robbed or misused.

Table 4.2. *Security requirements of the interfaces.*

Interface	Confidentiality	Integrity	Availability
U1	H	M	L
U2	L	H	L
U3	L	M	M

One important limiting factor for the HEMS is the cost; it can cost only cost that much money meaning compromises in many parts, also in security components such as firewalls. The HEMS will be accessible by many different vendors with different concepts of security. [13, pp. 57-58.]

Between HEMS and meter, the integrity of data is vital, as wrong data would have a straight impact on the system. The availability of the information is important, but not critical, since alternative means for gaining the information can still be used. Many stakeholders may need access to the metering data, increasing the cross-organizational security concerns. Some of the meters are located in unsecured locations, limiting the physical security. Also, Smart meters and the standards that they use are still relatively new, having possible vulnerabilities in them. Meters are constrained in their computational capabilites, and the key management of millions of meters is a challenge. [13, p. 63.]

The UI of HEMS will also handle some sensitive material that should be treated as confidential. However, there is no need for realtime information, and the availability of informatoin is not critical. The places of vulnerabilites and challenges are in wireless communications, and in key management [13, pp. 54-55.]. Table 4.2 above presents NIST´s security requirements for the three interfaces in question [13, p. 75].

The conclusion is that, according to NIST, the integrity of information is a number one priority. This is rather sensible, as wrong or false information would lead, in the end, to the system to operate falsely. However, especially from the end user's point of view, the confidentiality of information is also an important factor.

4.2.2 The assets

Adversaries attack because of the assets that the system possesses. These assets can vary from money to reputation. From the end user's point of view, the system handles a great deal of information about customers, keeping track of their electricity consumption, sensitive personal information and so forth. If this information is accessed by an unauthorized person or utility, it may be possible, for example to know when the user is at home, what is the user´s energy consumption behaviour and so forth. This information can be used by criminals to plan a robbery, police forces like the CIA to monitor users, adversary companies like Google to profile users´ needs and so forth. [14, pp. 19-32.]

Table 4.3. *The assets of the system.*

ID	Tangible	Intangible	Description
A1	Information		Information about customers may be of interest by many adversaries.
A2	Property/ people		Customers have a lot of different equipment to protect, like resources, home security equipment and such. Also, Smart Grid is for people and must not compromise human lives or their well-being.
A3		Feel of security	If the end users do not trust Smart Grid or feel safe at their home, this will ultimately destroy the implementation of SG.

Besides information, customers also have resources, devices and property that can be harmed, robbed, destroyed, or used without permission for various motives. An unauthorized use of user´s home devices may result in melting of fridge, or in the worst case, cause fires or other accidents that can take lives. Also, as the users' resources are part of controlling the grid, they might be attacked in order to cause trouble to the whole grid. HEMS will also provide the most accessible path to the Smart Grid, and thus, it will be under attacks.

Successful attacks can change the attitudes against Smart Grid, especially if people start to think that their security as well as dependability of their electricity is in danger. The feel of security can actually be one of the biggest assets that the end users have. The lost of trust and confidence on the system can result in many issues, for instance, avoiding the use of the equipment leading to the unsuccessful implementation of Smart Grid. Table 4.3 gathers all assets of the end users and categorizes them into tangible and intangible groups.

The third asset, feel of security, is rather connected to the other assets. In other words, successful attacks targeted to assets A1 and A2 can lead also to asset A3, even though not intended.

4.3 Characterizing the system

To comprehend exactly how a possible attacker could penetrate the system by, for example, manipulating the data, it is vital to understand the system more closely. Since all systems treat data, data flow figures are a very practical way of representing how the system works; where data comes from, where it goes to, who has access to it, and so on. [57; 58.] Figure 4.2 describes one possible way of how the information of end users is aggregated, and sent to the ICS. The figure does not take into account what happens to the data inside the ICS or aggregator.

.

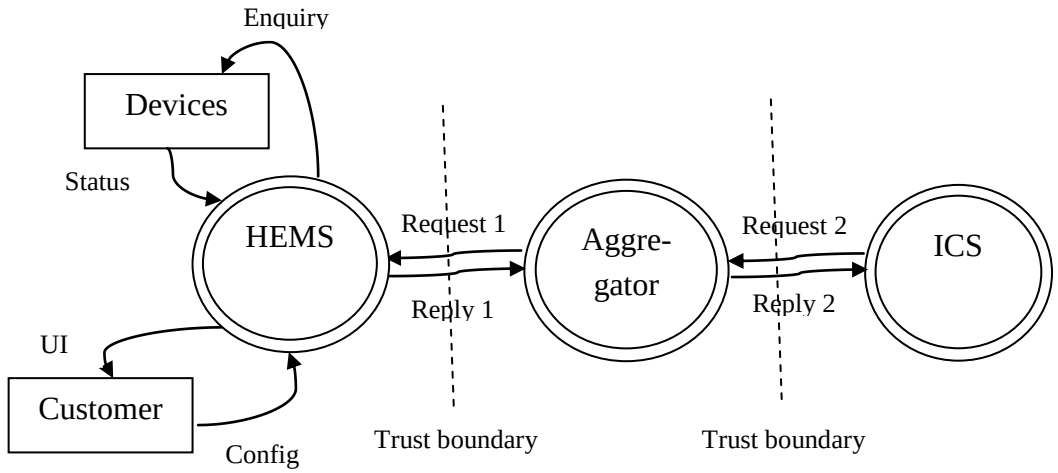

Figure 4.2. *The data flow of the demonstration system from devices to ICS.*

To make the data flow more complete the following lists describe what exactly the requests and responses could contain [53]:

Request 1; Messages from aggregator to HEMS:
- Parameter change
- Query to check if the communication and automation system are alive
- Distribution of contract and tariff data to resources
- Query of missing or bad quality data

Reply 1; Messages from HEMS to aggregator:
- Disturbance event (real-time data)
- Disturbance recording
- Monitoring of resources (real-time data)
- Statistics of resources
- EV started charging (real-time data)
- EV stopped charging (real-time data)
- Registration of new resource
- Customer query about its own resource

Request 2; Messages from ICS to aggregator
- Query to check if communication system is alive

Reply 2; Messages from aggregator to ICS:
- Disturbance report to SCADA
- Summary of real-time information about resources to SCADA
- Query to check if communication system is alive

As mentioned, this architecture is one possible solution. The business idea behind this model is that aggregator has some control over customers´ devices like, electric car batteries, and can thus provide this controlling service to grid operator.

4.3.1 Implementation of the system

There are many ideas and plans of how the information infrastructure of Smart Grid can be carried out. Especially, the collection, aggregation, and distribution of information from customer domain are still open questions. One possible solution for information infrastructure is a decentralized plan, where the idea is to distribute the decision making devices to many levels. The decentralized plan enables local generation and consumption of energy, as well as other functionality.

In the decentralized model, the aggregator plays an important role. The aggregator itself can be divided into several software components that are running and working in different computers, and in different places of the grid. LV automation system is one very plausible place for the aggregator component, having connections with the HEMS, and with other main aggregator components. Especially in a rural environment, these centres might be easy targets for adversaries, and require some sort of surveillance. In order to communicate with each other, these components need a network.

In Finland, many entities, such as electric distributor companies and teleoperators have been installing a great deal of optical fibre. In fact, Finnish communications regulatory authority, FICORA, set a goal that by the end of 2015, a national broadband network will be installed [59]. As HEMS will be at the customer´s premises, wired solutions, such as cable or optical fibre, provide a natural way for HEMS to be connected to other components of the Smart Grid system. However, there are also components, for instance, smart meters, in the Smart Grid that will use additional techniques for communication. In Finland, for example, all smart meters use tunnelled general packet radio service (GPRS) which the ISPs are providing to the DSOs [60]. This threat model concentrates on the connections of the HEMS.

Since the HEMS will utilize the Internet as communication media, it might also act as an enhanced WLAN router. In order for customers to easily manage and configure both WLAN settings and home devices, the HEMS will offer a UI [53]. There are vulnerabilities with WLAN, even when configured and used properly. The risk differs greatly depending on the location and type of use. For example, using WLAN in households in a rural area is a bit different than using it in apartments in cities. Despite this, the vulnerabilities and threats remain the same; only the likelihood differs. Same goes for other wireless networks that the HEMS provides, such as Z-Wave among others.

In apartment buildings, the network structure is a bit different from private households. It is typical that the communication and data of all apartments are gathered, and sent via optical fibre that comes into the building. The communication technique to each apartment can vary. Home PNAs, for example, are used in many places utilizing the old installed twin cables [61]. The Smart Grid implementation in these kinds of environments can be done utilizing the already existing network structure or with, for example,

using GPRS. However, with the Smart Grid too, the information is first gathered from all the apartments, and then sent forward, even with GPRS technique. In any case, the information is sent using the same cable or optical fibre that the Internet uses. From an information security point of view, this may raise new threats, such as possibility of information leakage via eavesdropping.

4.4 Determining threats and vulnerabilities

Threat is a potential attack that, by exploiting vulnerability, may harm the assets. Vulnerability, on the other hand, is a flaw, or weakness in a system that could be exploited to violate the security policy of the system. The HEMS is the most alluring and probably also the easiest path for adversaries to penetrate into the Smart Grid system, and thus also will be subject to a variety of attacks. From the end user point of view, this creates the biggest threats, and the main attack vectors.

The attack vectors presented here describe three situations in which the assets could be reached: the HEMS crashes, works incorrectly, or loses sensitive information. The root cause to these situations can be found by following the attack trees to the last node (path marked with red colour). These attack trees do not cover all possible threats, but concentrate on the most likely and severe ones. Same applies with the vulnerabilities behind the threats. Neither do these threat trees give very specific threats, but leave them on a higher level. Each of the root causes could be investigated further, but the idea of this threat model is to remain on a more general level.

4.4.1 HEMS crashes

The most straightforward and visible threat for the system is a situation where the HEMS stops working. The HEMS may fail due to unintended reasons, such as a lightning breaking the equipment, or intended reasons, such as DoS attacks. Unavailability of the HEMS can cause unexpected situations. For example, if the HEMS has been instructed to turn off the fridge for a while, and after that the HEMS will be out of service, the fridge continues to stay off. Figure 4.3 presents the attack tree of this threat.

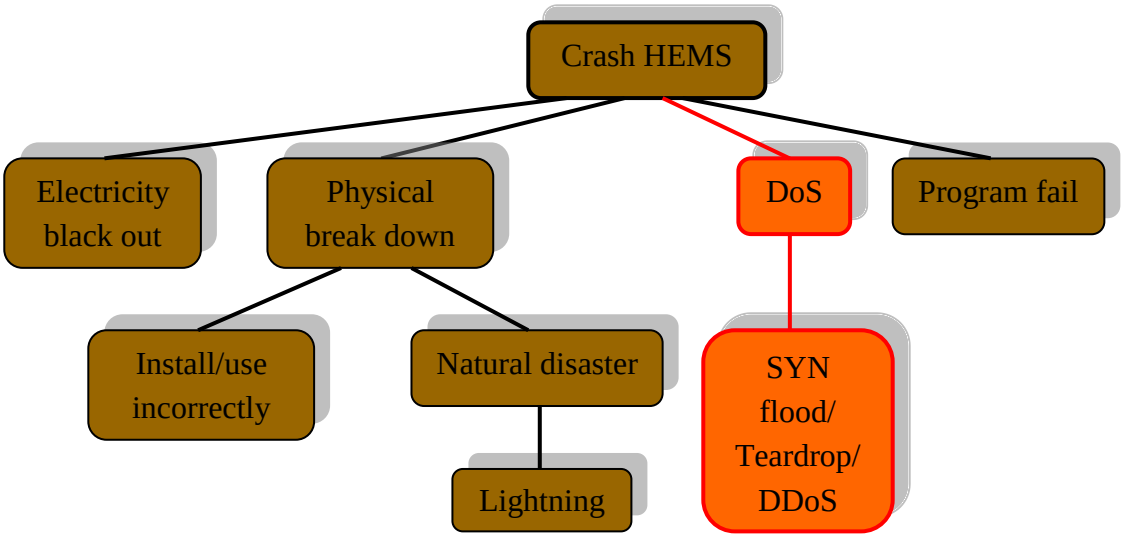

Figure 4.3. *The attack tree of HEMS crashes.*

From the reasons that can cause the HEMS to be unavailable, the DoS attacks are the most important ones to address. This is because they are not as obvious to people as an electricity blackout, or a physical break down. Also, defence against DoS attacks is much harder, sometimes even impossible. There is a variety of different types of DoS attacks. The attack tree represents only a few which are relevant in this environment.

The vulnerabilities behind DoS attacks vary depending on the situation. In SYN flood, for example, the attacker uses the TCP three-way handshake wrongly by only sending a synchronize (SYN) message to the server, but not responding to the server´s acknowledge (ACK) messages [62]. The most recent DoS vulnerability has been found in the secure sockets layer (SSL) protocol, where the attacker demands renegotiations of encryption keys, resulting up to 1000 parallel connections between client and server [63].

4.4.2 HEMS works incorrectly

Another threat situation is if the HEMS works improperly; for example, it turns on the Sauna even though not supposed to, or sends wrong information to higher level equipment such as the aggregator. The causes for the HEMS to malfunction are unintended and intended code-based errors, and adversaries´ attacks. Figure 4.4 presents the attack tree of this threat.

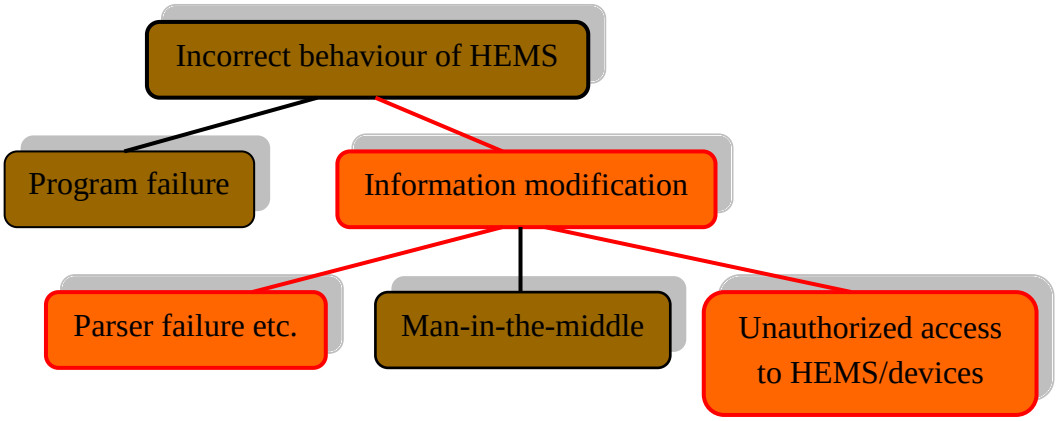

Figure 4.4. *The attack tree of HEMS works incorrectly.*

The modification of information is a serious threat that must be addressed, as it can be harder to notice than a program failure. If, for example, the metering information is slightly changed, it can take a long time to spot it, and may result in financial losses for a customer or for an electric company. The modification of data includes bad messages, situations where, for example, the parser fails, and also intended unauthorized modifications. It must also be remembered that this attack tree applies to the situation where information comes from a higher-level to the HEMS, for example, from an aggregator

Adversaries can manipulate data if they have access to equipment such as meter or HEMS, or if they perform a MITM attack. If no encryption or authentication is used, performing an MITM attack is easier. The vulnerabilities behind parser failure are most commonly due to data validation process. Attacks, for instance, SQL injection, exploit these issues, trying to gain access to sensitive information for instance.

One of the biggest threats that the system poses is that the HEMS is accessed by an unauthorized person. There are several ways for this to happen; hacking the Web interface via browser, using vulnerabilities of wireless technologies, using the end user's personal computer to access HEMS, or physically accessing the HEMS. The adversary might be able to not only control the home devices, but also manipulate metering information that is sent to the aggregator. The adversary may also gain access to sensitive information. Following Figure 4.5 presents the attack tree of this threat.

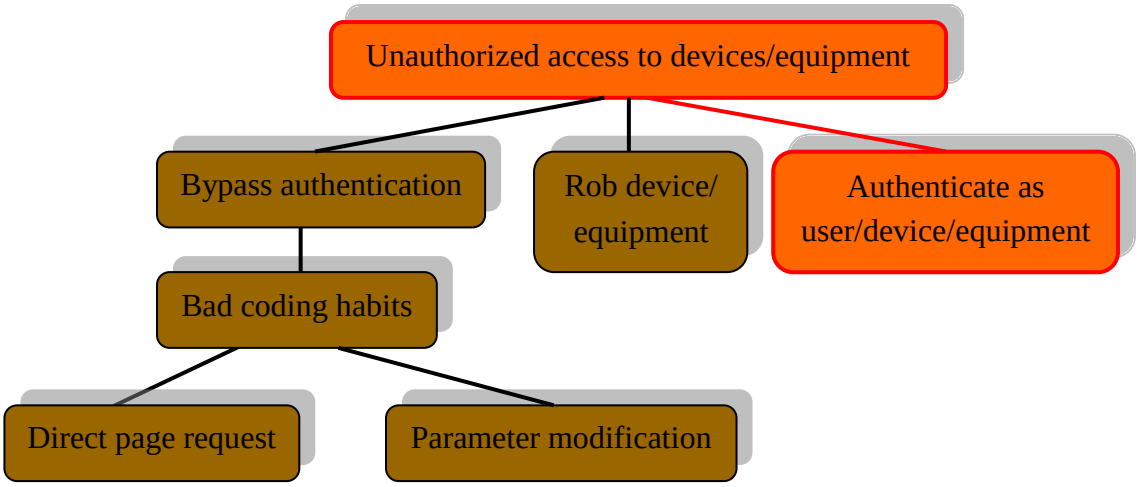

Figure 4.5. *The attack tree of unauthorized access - HEMS.*

The bypass of authentication is possible due to the vulnerabilities in planning and coding processes. Most of them can be avoided by using safe coding principles. It is more difficult to protect the system against identity frauds. This is due to the fact that end users are the information security threat number one, and due to the restrictions that some of the equipment pose, like cost efficient solutions, and memory or central processing unit (CPU) constraints. Figure 4.6 below presents how an adversary might learn the credentials of the end user, device or equipment.

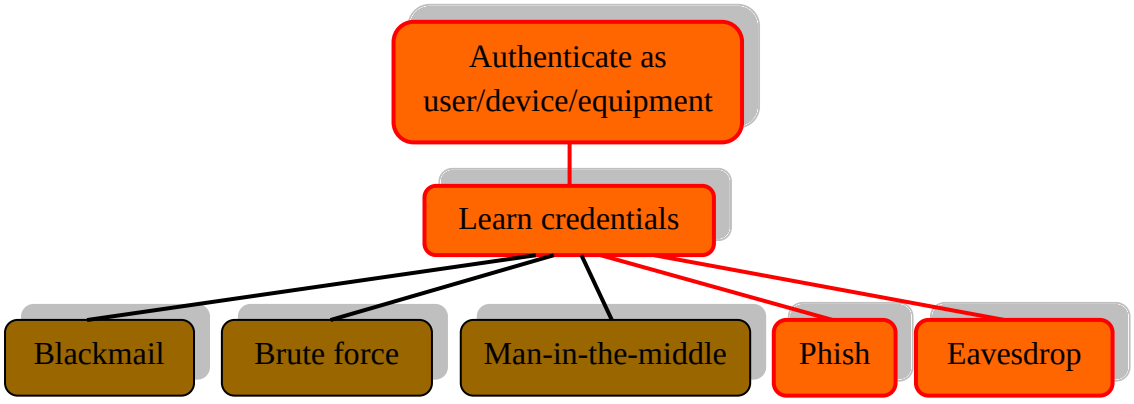

Figure 4.6. *The attack tree of unauthorized authentication – HEMS.*

Regardless of the system, the human-factor is always its weakest point, and poses the biggest vulnerability. People are, in the end, lazy, ignorant, unaware, busy, and rash, and many other things that make exploiting them an easy target. In the long run, even the most conscientious people will break the security instructions and procedures of the company. In the HEMS, the biggest effect of the human-factor is in the UI. Usernames and passwords are very common ways of identification and authentication of the users. However, these kinds of systems do not work as well as people think they do. Firstly,

there is a contradiction between a good password and one that users remember, or even use. Dictionary attacks can be effective against a poor and even not so poor a password, as the computing power has increased significantly. Nowadays, passwords can be brute-forced. For example, with 400 MHz Quad Pentium II, every possible seven character password can be tried in 480 hours using the L0phtcrack program. Also, there are users that make things even worse by choosing the same password from one application to another, or are willing to give the password away to others too eagerly. Other credentials have vulnerabilities as well. For example, if certificates are used, the most difficult problem to solve is the safe management of the keys. Even users that are more aware of information security can be used to penetrate the system. For example, it is very much possible and rather easy to get some malware on one´s computer. These malwares can spoof the user´s credentials and so forth. [15, pp. 136-141.]

There are solutions to make the use of a password more secure; this can be done, for instance, by locking up the system after a certain amount of bad passwords. However, this must be done in discrete manner, or it can lead to another type of DoS attack.

4.4.3 HEMS losses sensitive information

One of the assets that the end users have is information. The loss of sensitive information is a serious threat that may result in several issues. An adversary needs only to be able to see the sensitive information. This can be done through MITM attacks, gaining access to device or equipment, bribing some person or utility that is handling the information, or eavesdropping. Figure 4.7 below presents the attack tree of this threat.

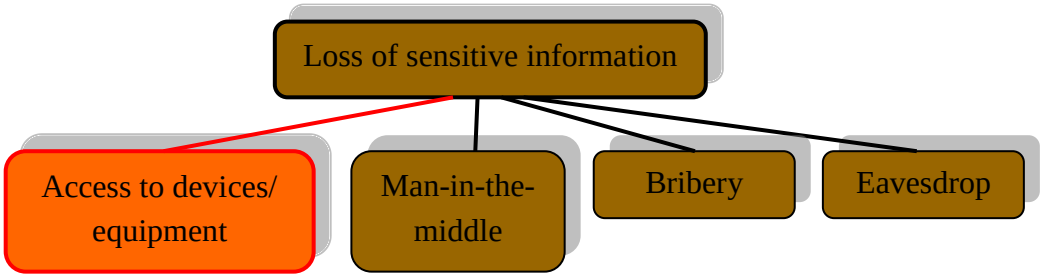

Figure 4.7. *The attack tree of loss of sensitive information – HEMS.*

Presumably many utilities will be interested in information on customers. This may lead to the point that, for example, some news agency will bribe someone from the aggregating company to give sensitive information. However, if the punishment of such a crime would be high enough, people would not be so eager to take the risk. MITM attacks and eavesdropping are both dangerous attacks. Encryption of information will, however, prevent easy access to data.

5 REVIEW OF LABORATORY DEMONSTRATION

The purpose of this chapter is to review the TUT demonstration equipment from a security point of view. This is very important in order to comprehend which security issues apply, and how adversaries might exploit the system.

The main focus of this thesis is from the interface of the ICS downwards, all the way to end user's devices. The ICS itself is left to less attention. This thesis will also neglect analysis of communication technologies, such as PLC, or long term evolution (LTE) used between devices, and the HEMS or other Smart Grid components. ThereGate will aim to be independent from used wireless technologies. In the current status of demonstration, only the Z-Wave and WLAN are supported, but in the future, other techniques will be supported as well. Wireless communication methods, such as Z-Wave or WLAN, are, in the end, just using different media than the wired ones. Although wireless technologies have their own characteristics, the information security problems are mostly the same, as they do not alter according to the used media. For this reason, analysing wireless technologies is left to the background, and only Z-Wave and WLAN security issues are briefly analyzed.

The analysis presented here will not discuss users, procedures or such, but instead focuses on the technical part. The information presented in this thesis regarding these components is based on current versions of the equipment and software.

5.1 Components

The laboratory demonstration environment consists of ICS (SCADA/DMS), OES, Agent, Northbound Mediator, and ThereGate [53]. ICS and OES are already commercial, full-fledged software, whereas ThereGate, Agent, and Northbound Mediators are still under development. Figure 5.1 presents the overall layout of the demonstration with components and used platforms.

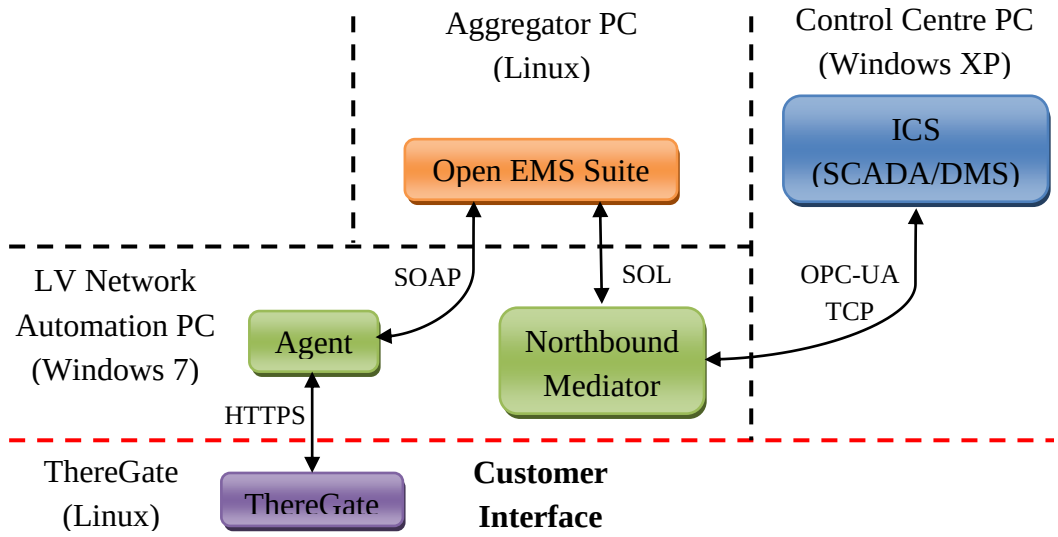

Figure 5.1. *The layout of demonstration environment consisting of computers, components and interfaces.*

As illustrated, ThereGate and OES run on Linux, whereas both mediators – Agent and Northbound – run on the same computer with Microsoft Windows 7. ICS runs on Windows XP. From an information security point of view, the most critical part of the system is the part that is the most public, and has a variety of different users. In this case ThereGate is the customer interface, and securing ThereGate should, thus, be the number one priority.

5.1.1 ThereGate

Basically, ThereGate is an enhanced WLAN router with firewall and Network Address Translation (NAT), port forwarding, and media access control (MAC) address filtering. It runs on an embedded Linux OS, and communicates with home devices, using home automation communicating protocols. In the demonstration, however, no devices are connected. The hardware of ThereGate consists of a processor (533 MHz), 256 MB DDR2 memory, 6 GB of internal flash memory, and a trusted platform module (TPM) v. 1.2. It includes four USB 2.0 host ports, an SD memory card reader, and an Ethernet switch with four LAN ports, and one WAN port. ThereGate has an external power source, but can run on batteries as well. [53; 55.]

ThereGate has connections to the Agent, and it provides a graphical UI (GUI) for the user to monitor, add, and control home devices, and configure the WLAN router settings. The connections to the Agent and the GUI are done by using hypertext transfer protocol (HTTP) application programming interface (API). This connection uses HTTP with SSL/TLS to protect the information. ThereGate can also be accessed remotely with a terminal using a secure shell (SSH) connection. In order for a user or an application to access ThereGate, they need to have proper credentials (username/password combination). [53.]

The connection to the Agent uses a request/reply message pattern. This means that the Agent must start the communication, and ThereGate cannot send anything spontaneously to the Agent. This is why there needs to be a time-based communication structure; the Agent requests raw, real-time data from ThereGate every minute, using GET request. The data is expressed in JavaScript Object Notation (JSON), and contains information about the customer, devices, meters and so on. [53.] Figure 5.2 below presents the core components and protocols of ThereGate.

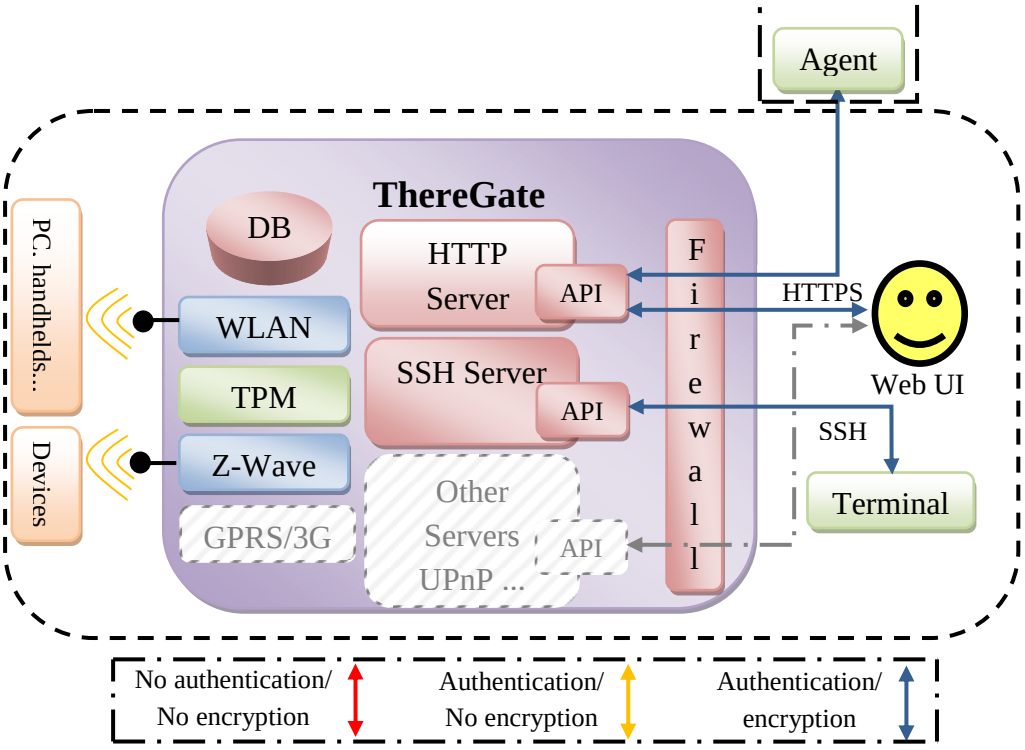

Figure 5.2. *The layout of ThereGate with components and used protocols.*

The version of ThereGate presented in the above Figure is used in the demonstration. However, in later versions, ThereGate will most likely include other components and servers as well, for instance, a universal plug and play (UPnP) server. Adding components like UPnP to ThereGate will radically change the situation by creating new information security threats. Thus, after every change made to ThereGate, a new evaluation of information security must be made.

5.1.2 Aggregator

The aggregator can be divided into three software components: Agent, OES and Northbound Mediator. OES is the aggregation centre where all the information is gathered. Agent and Northbound Mediator are just adapters to connect the ICS to OES, and OES to ThereGate. [53.]

The Agent itself consists of three components: HTTP Client, an extensible mark-up language (XML) file generator, and an NE3S/WS interface. The HTTP Client is used to

communicate with HTTP Server of ThereGate. This communication uses HTTP to transmit the messages, and also provides also possibility to encrypt the data with SSL/TLS. The messages from ThereGate are in JSON file format. However, in OES, the configuration management (CM) and performance management (PM) adaptations define the structure details of files that can be accepted to OES; only certain type of XML files – Open Configuration Data Standard (OCoS), and Open Measurement Standard (OMeS) files – are accepted. In order to make such files, Agent first uses JSON-lib library to parse JSON files and extract useful values from them, and then creates OMeS and OCoS files. In this demonstration, the power demand value is treated as PM data, and used to create an OMeS file, information such as timestamp, status, indoor-temperature, and so forth being treated as PM data, and used to create an OCoS file. If there is need to update the values, the XML files are attached to simple object access protocol (SOAP) requests, and sent to Mediation Framework (MF) of the OES, using an NE3S/WS interface. SOAP can be used in combination with a variety of Internet protocols. In the case of the demonstration, SOAP uses HTTP for message negotiation and transmission, and XML for message formats. The SOAP messages are not encrypted, but are in a plaintext format. Before sending any information, authentication is required; first, MF discovers and registers the Agent during which the Agent is working as a Web Service (WS) Server. When the registration is over, the Agent begins sending SOAP requests to MF, and works as a WS Client. However, there is no specific authentication for Agent; the Agent ID is its IP address, and the Agent key is allocated by the OES. [53.]

The OES has connections to both Northbound Mediator and the Agent. It also has a Desktop UI for the software developers and staff in the aggregation centre that can be used via Web Browser. These users can be authenticated, and their access controlled with OES user management. All the messages between OES and Desktop UI are transmitted over HTTP, and encrypted by SSL/TLS. To the Agent side, the connection is done by using MF, which works in the manner of a middleman, allowing the fact that the Agent does not have to be concerned about the OES structure. From the MF, the XML files divided into measurements and control information are populated into the databases accordingly. The PM data is later handled by the OES PM Platform to make an aggregation calculation. The CM data is later handled by OES Managed Object Framework (MOF), which enables presenting needed information on the OES desktop UI. [53; 54.]

The function of Northbound Mediator is to work as an adapter between the OES and ICS systems. Each minute, Northbound Mediator retrieves and aggregates raw data directly from the OES PM Database by using PM SQL API, which has read access only to the data. The Northbound Mediator is authenticated with a username/password combination when establishing connection to the database. However, no encryption is used at this point. In order to communicate with the ICS, Northbound Mediator acts as openness, productivity and collaboration unified architecture (OPC UA) Client, and sends the sum of power demand values to the ICS over an OPC-UA TCP protocol. The OPC

UA client has been made using Open source OPC Client from Prosys OPC UA Java SDK. This connection is using neither authentication of client, nor encryption of data. [53.] Figure 5.3 below presents the components of the aggregator, and how they are connected.

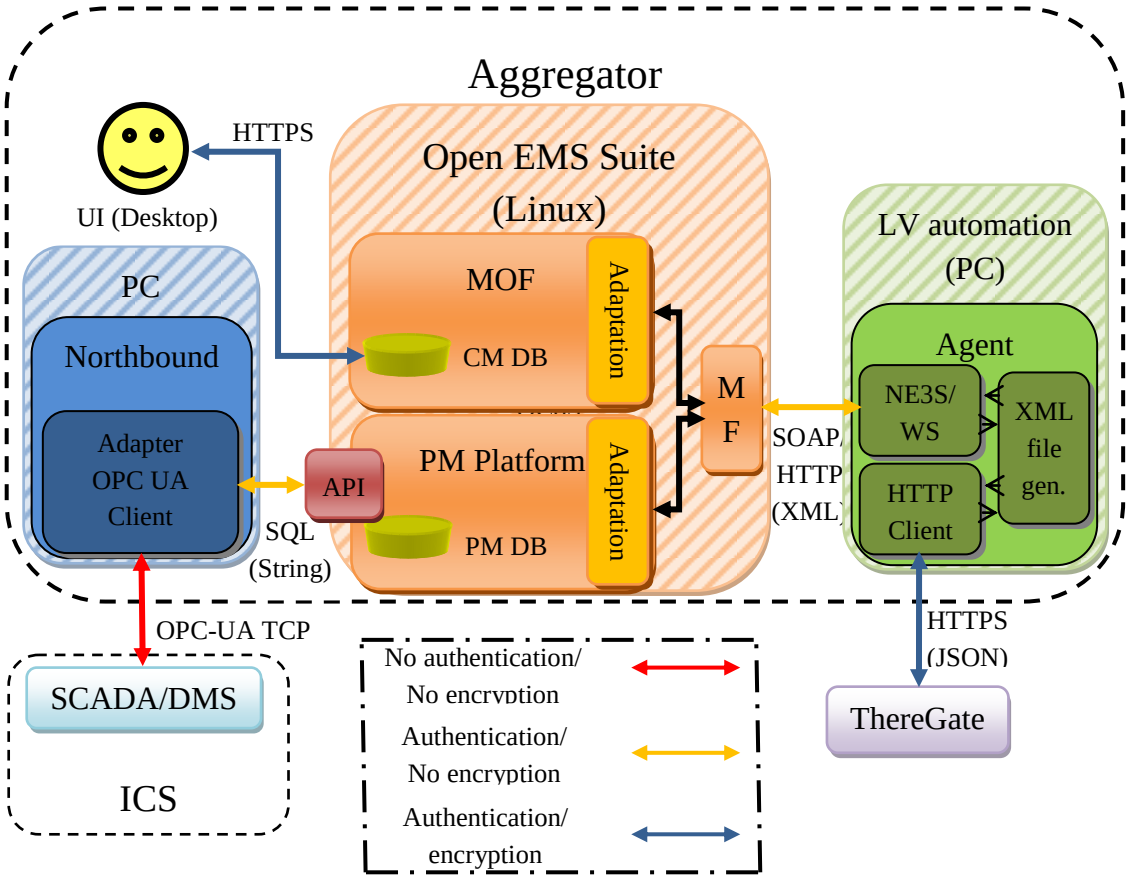

Figure 5.3. *The layout of the aggregator with mediation components and UI.*

As the OES is already developed software, more specific information about its architecture and building blogs is difficult to require. However, even though not all information is available, a good deal of information analysis can be done, as the interfaces are the most critical part of any system.

5.1.3 Industrial control system

The ICS runs on the Control Centre PC (Windows XP), and consists of DMS and SCADA. These two programs have built-in interfaces, and are designed to be used together. The data transfer between DMS and SCADA is done by the OPC Data Access (DA) and OPC Alarms & Events (A&E) interfaces, so that the servers are on SCADA's side, and the clients on DMS's side. At the current state of the demonstration, the ICS cannot send any messages to ThereGate, and its purpose is only to supervise and monitor the system. However, in the future the ICS will also have the ability to send straight commands to lower-level equipment. [53.] Figure 5.4 describes the overall layout of the ICS.

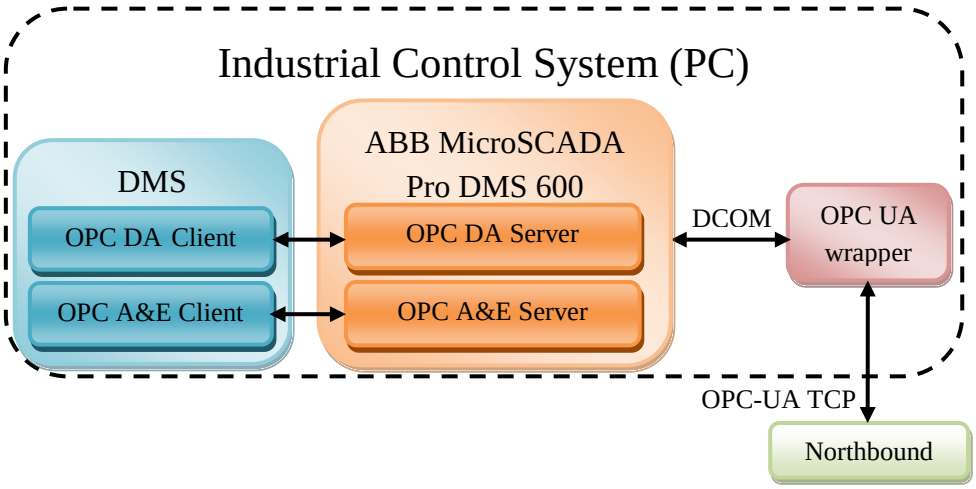

Figure 5.4. *The ICS consisting DMS, SCADA and OPC UA wrapper.*

The OPC UA wrapper has already been developed, and the main focus from the demonstration point of view is on the interface between the OES and ICS. In addition, in the case of demonstration, the entire ICS system will be working only on one and the same computer (PC), which may not be valid in real Smart Grid environment.

5.2 Information security analysis

The vulnerabilities found in the demonstration environment are divided into three groups: vulnerabilities in hardware, software, and in protocols and communication technologies. However, the hardware part is left to less attention, the concentration being on software and communications.

5.2.1 Vulnerabilities in hardware

Embedded systems, such as ThereGate, often have physical constraints, which make them more vulnerable. For example, limited processing power can result in DoS. However, probably the biggest threat concerning ThereGate´s hardware comes from the fact that in the future these equipments can be bought and examined in home with all the time and privacy. After a vulnerability has been found, it can be used to attack the system.

ThereGate has many physical ports, such as SD Card and USB ports. These interfaces enable using rogue devices, especially if not configured right. If, for example, a customer´s memory stick is infected with malware, it spreads to ThereGate when the user puts the memory stick in the USB port of ThereGate. Disabling all ports as a default, and denying auto-open feature of memory sticks could prevent at least some cases. This, nevertheless, might have a negative effect on the using experience. ThereGate will also be subject to electricity blackouts and such. If, for instance, a home automation security system is integrated to ThereGate, electricity blackouts can cause

them to fail. However, ThereGate already has a backup battery place installed in these kinds of situations.

ThereGate includes TPM, specified by Trusted Computing Group. TPM is a secure crypto processor that offers secure generation and storing of cryptographic keys, and limitation of their use. It is also used to protect passwords from dictionary attacks, still allowing a reasonable number of tries. [64; 65.] However, there are also vulnerabilities in TPM. These include, for instance, cold boot attacks, where encryption keys are retrieved from the OS after using a cold reboot to restart the computer [66].

Embedded equipment is not the only thing that suffers from computing constraints. Heavy software and encryption can bring down even new computers. In the demonstration environment, software like OES and ICS will require a lot from the PC they are running on. If the computers are slow, they are more exposed to DoS attacks.

5.2.2 Vulnerabilities in software

The OS is the cornerstone of every system. However, every OS has security holes, some more than others. Linux OSs are regarded to be more secure than, for example, Windows OSs. On the other hand, this might lead to a false feel of security. The vulnerabilities of OSs are well-known and compromise the entire system, whereas updates fix old, and introduce new vulnerabilities. [67; 68.] Using different OS in different parts of the system creates vertical safety, as the adversary cannot use the same OS vulnerability in other components of the system. If ThereGate, for example, had some vulnerability in its Linux OS the same vulnerability could not be used to attack, for instance, the Agent.

The OS creates a platform over which other software is working, providing more services and such. These additional software also have vulnerabilities, some of which are more critical than others. Just like in the OS, it is vital to know the version and patch level of the software, as their vulnerabilities are well-known. It is also important to know how the software is configured: Bad configuration makes good software risky, whereas good configuration mitigates existing security vulnerabilities in the software.

These vulnerabilities do not apply merely to servers, but also the client software. According to SANS, client side attacks are nowadays among the most common attacks. Vulnerabilities in client-side software, like browsers, are exploited to compromise computers that have Internet access. The simple act of going to the infected web site may be all that is needed. [67.] Firewall, if configured right, can protect the system, and hide known vulnerabilities. The demonstration environment includes both servers and clients, among other software, each of which possesses possible vulnerabilities.

The vulnerability does not always have to be a bug in the server or such. It can also be a matter of how the system works, and what techniques it uses. The Agent, for example, does not verify in any way the content of the JSON files: if the given JSON file follows the JSON-lib grammar, it will be accepted. What is more, there is no validation of data in any part of the system. It is possible that this feature could be used to make data injection type attacks, resulting in loss of sensitive information, DoS, or even accessing the Agent, for instance. Actually, manipulation of data is probably the most lur-

ing possibility for the adversaries, and also the most dangerous for the system: changing one´s energy bill can be a motivator, and incorrect data can ultimately cause Smart Grid to work wrongly. [69.]

5.2.3 Vulnerabilities in protocols and communication technologies

One of the main security issues regarding ThereGate has to do with the vulnerabilities of the wireless technologies. Z-Wave, for example, only has data encryption in version 4 [70]. Moreover, the level of encryption cannot in any case be very high, as the mesh network would otherwise suffer too much latency. This means that adversaries could easily learn one´s Home ID by, for instance, using a sniffer tool, and gain access to the Z-Wave network. In that case, it would be possible for the adversary to monitor the user´s way of living, violating privacy, or for example, switching lights on and off. Moreover, as the product family of Z-Wave continues to grow, other components, such as door locks, are implemented, which creates new kinds of threat scenarios [71].

WLANs are also prone to security vulnerabilities [72, pp. 25-28]. Many of these can be taken care of by applying a little effort on configuring the WLAN settings. However, some vulnerabilities, for instance, some DoS attacks, are hard, or even impossible to mitigate. As all information goes through air, eavesdropping, and conducting MITM attacks are serious threats. On the other hand, the propagation areas of both Z-wave and WLAN are rather limited, which requires that the adversary is nearby. Moreover, encryption of data is an efficient and easy way to prevent these types of attacks, even though most of the WLAN encryption can be cracked rather easily [72, pp. 32, 36]. ThereGate supports Wi-Fi protected access (WPA) 2 encryption which is, at the time when this thesis is written, the strongest and most recommended form of encryption and authentication. There are, nevertheless, vulnerability holes even in WPA2 [73] and the recommendation is to use it with other methods, such as extensible authentication protocol (EAP).

The hypertext transfer protocol secure (HTTPS) in this demonstration environment is using transport layer security (TLS) and SSL. This, however, does not automatically mean secure connection, as there are also vulnerabilities in TLS and SSL protocols. One found vulnerability of TLS is in its renegotiation feature, which allows a client and server, who already have a TLS connection, to negotiate new parameters, generate new keys and so on. An attack on this renegotiation logic may result in a MITM attack, where the attacker can inject data in an encrypted session, and it will be treated by the server as if it came from the client. Thus, a violation of the integrity of information would take place. The impact of this type of an attack depends on the application protocol running over TLS, in this case HTTP. The initial authentication of a client is done with a username/password pair. This authentication state is then kept on with HTTP cookies. It is possible that an adversary could exploit this issue by sending a partial HTTP request prefixed to the client´s real request. A similar type of attack is possible with certificate-based client authentication: it is common that the server lets clients connect and request a resource, after which a certificate is asked. Similar MITM attack

would be possible to do, in this case, by using the renegotiation vulnerability. However, the attacker would not see any sensitive information directly, as it is sent encrypted via server and client. [74; 75.]

ThereGate also includes SSH connection to enable remote connections. SSH provides authentication and secure communication over insecure channels. There are, however, vulnerabilities, like buffer over flows in many sold SHHs, especially in the older SSH1 version. These vulnerabilities allow an attacker to execute arbitrary code with the privileges of the SHH process: in Windows, SHH runs with system privileges and in UNIX with root privileges. [76.]

The XML documents travel from client to server in the shape of SOAP request. XML is then processed within the web service, opening it to XML-based attacks. The three most common attacks against web service are buffer overflows, XML injections, and session hijackings. In buffer overflow, the adversary can craft XML data that is too long, or contains malicious coding, like calling upon itself repetitively. These attacks result, among other things, in DoS, and loss of information. In XML injections, the adversary tries to exploit the incorrect data validation by using SOAP messages to create XML data which inserts a parameter into an SQL query. There are also other types of attacks that exploit the incorrect data validation. For example, in Schema poisoning attack, the adversary tries to change, or replace the XML schema in order to allow the parser to process malicious SOAP messages and XML files. Adversary might also gain control of some user´s session state by, for example, sniffing SOAP messages, and stealing a session ID. This information could then be used to access the application with the user´s privileges. [77; 78.]

OPC UA provides a means to authenticate users, and encrypt the content. Nevertheless, the OPC UA protocol does not require authentication or encryption as compulsory. From the information security point of view this is really bad, since now the developers and companies involved in OPC UA do not use it, as it is not obligatory. [79.] In the demonstration environment, neither authentication nor encryption is used in the OPC UA protocol. Moreover, the specification accepts self-signed, and other certificates without any hesitation.

6 DETAILED ANALYSIS AND TEST RESULTS

This chapter presents three different scenarios of the ownership of ThereGate, analyzing and testing them. In the analysis part, most critical interfaces of the system are found, whereas in the testing part, interfaces will actually be tested, and the results analyzed. The testing is done in cooperation with Codenomicon Ltd. (Oy), who provides very useful testing software.

6.1 Test case analysis

The Smart Grid demonstration environment, described in chapter three, presented the question about the ownership of ThereGate with three possibilities: ThereGate is owned by

A. User
B. Internet Service Provider (ISP), or
C. Distribution System Operator (DSO)

As one of these scenarios will actually come to use some day, it is interesting, and important to understand what information security issues each possibility brings along. This can be done by first analyzing each scenario in order to recognise the interfaces that are under danger, and analyzing how this affects to the functionality of the system. The testing of the interfaces will help to find vulnerabilities indicating what components of each interface need to be protected in order to protect the whole system.

6.1.1 Customer owns ThereGate

It is plausible that the customer will have to purchase HEMS equipment, such as ThereGate. This means that it is the responsibility of the customer to carry out the information security of the equipment. This has been the case in many situations with cable and Ethernet modems in Finland. Adding more responsibility to end users is in some cases necessary. For example, in Finland a new law has been passed that makes the use of unprotected WLAN legal [80]. In the Smart Grid environment, however, ThereGate is also used by other entities, and not only the customers. This creates a more complex environment, including certain requirements for confidentiality, integrity and privacy. In what way would it be possible to engage users to take care of the information security of ThereGate? Should there be more laws or other financial penalties, if ThereGate security has been neglected? What about those users who want to use

ThereGate in criminal ways? How much can ISP or DSO, who rely on the integrity of the information of ThereGate actually trust ThereGate, if it is managed by users?

From an information security point of view, this case model allows users to modify, and temper ThereGate as they wish. It will make it more alluring to attempt to modify, for example, consumption information, in order to gain some profit. One of the most popular targets in the system is the OES database, as it has all the user information. What is more, in the current version of the demonstration system, the information from ThereGate is not validated at any phase of the system. This makes attacks like data injection easier to conduct, making it possible to actually manipulate that consumption information, for instance.

Even if all users would be pure hearted, the level of security varies a great deal, as people´s knowledge and know-how of information security varies too. For these reasons, ThereGate cannot be trusted, and should be treated with suspicion. The main attack vectors come from wireless technologies, GUI, and the human factor, having multiple access routes. The interface under immediate danger is ThereGate´s GUI, as it can be accessed via Internet. Also, as ThereGate cannot be trusted, the interface between ThereGate and the Agent is under danger. As there are not many security features on the higher levels, the whole system can be considered to be under danger.

There are several ways of breaking these interfaces, and influencing the system that have different results. The vulnerabilities, for example, in WLAN, Z-Wave, passwords, authentication, encryption, browsers and so forth, are the main access points to the adversaries. Access to ThereGate gives the adversary a chance to modify home device settings, possibly causing damage to the premises, like melting the fridge. The adversary may also be able to access classified user information like the social security number, and alter the information that is sent to the Agent, resulting in manipulation of controlling, billing, and really any service that uses that information. It may also result in the adversary gaining access to Agent as well.

6.1.2 ISP owns ThereGate

Another plausible scenario is that some ISP, like TeliaSonera, owns ThereGate. This means that the ISP is responsible for the safety of ThereGate. Practically, this means that there is only that much that a customer can configure, probably not much more than certain WLAN settings. This way ThereGate will be a part of the ISP´s information security system.

From an information security point of view, this scenario offers a better level of information security for users and other entities interacting with ThereGate. Nevertheless, it is not impossible that adversaries manage to penetrate ThereGate even when an ISP owns it. Nevertheless, when an ISP is in charge of the information security of ThereGate, it will be more secure than it would be in the hands of the end user on average. On the other hand, when an ISP owns ThereGate, end users do not have much configuration opportunities, such as turning off WLAN, which may, in some cases, worsen information security, or at least upset people. Additionally, since it is in the nature of humans to

try and bypass restrictions one way or another, ThereGate will provide an alluring challenge.

The main attack vectors of this scenario come from the GUI of ThereGate, and from the wireless technologies used in ThereGate, such as WLAN and Z-Wave. The human factor is also relevant in this scenario, as criminal users are considered as insiders from the ISP point of view. In other words, the interface between ThereGate and the Agent can also be under attack.

It is also possible that ThereGate is owned by the customer, but managed by, for example, the ISP. This is the case, nowadays, in some cable- Internet/television modems that are provided by ISPs; Elisa Oyj, for instance, offers a service that includes the modem, but there are only few things the customer can configure [81]. On the other hand, the customer can buy a similar modem from the store to be able to have more configuration options, and modify the modem, but the ISP will force their own, daily firmware updates to every modem anyway. This way, although the customer owns the modem and can even do some modifications, the ISP is still controlling it, at least on some level. From a security point of view, this situation is very close to the one in which the ISP owns ThereGate.

6.1.3 DSO owns ThereGate

The third option is that ThereGate is owned by some DSO, meaning that the information security is the DSO´s responsibility. A similar situation can be found in the AMI architecture, where the AMI meters are in the premises of the customers, but owned by DSOs. Old electric meters have had seals to inform the DSO if a violation has been made. Same kinds of seals could be applied to ThereGate as well. Also, as new meters are ‘smarter’, other types of security features can also be added; for instance, logging events. [82.] However, in the manner of AMI meters, ThereGate would also require the services of some ISP in order to communicate with other systems.

From an information security point of view, this situation is rather like scenario B, where an ISP owns ThereGate. The customer still does not own ThereGate, and has a limited access to it, but on the other hand DSO needs to trust on the ISP providing communication methods. In other words, DSO buys communication service with security features from the ISP. However, as ThereGate is in this case not part of the ISP´s security plan, the ISP will simply do things that are mentioned in an agreement between the DSO and ISP.

These services might include a straight VPN from ThereGate to ICS system, for instance. If penetrated, an adversary would have a secured communication path to the other side of the VPN tunnel inside the DSO network! The interfaces under attack in this scenario are pretty much the same as in scenario B, but the risks are now part of the DSO´s security system.

6.1.4 Conclusion

It is clear that, in every scenario, ThereGate plays the most significant role in securing the system. Also, the interface between ThereGate and the Agent is very important. Depending on the scenario, the responsibility of securing ThereGate and the interface between ThereGate and the Agent alters, but the fact is that they need to be secured. As the role of ThereGate is so significant, it is not likely that scenario A, where customer owns ThereGate, is going to materialize. The difference between scenarios B and C, from the information security point of view, is rather small.

Securing ThereGate can prove to be a difficult task. Being the interface for normal people to Smart Grid, usability factors also play an important role. As there is a variety of users, it is plausible that different types of packages need to be offered to satisfy different needs. In each offered package, information security must be a factor as important as usability.

6.2 Testing plan

The idea of testing is to find vulnerabilities in the application and, moreover, to understand the root cause behind these vulnerabilities. According to OWASP testing methodology, testing should not only addressed equipment, but also the people using the equipment, their methods, and so forth. [83.] However, in the scope of this thesis, only equipment is going to be tested. The testing will be done more from a vulnerability assessment point of view than that of penetration testing. Thus, using tools like Metasploit are left to less attention, and the focus is on finding vulnerabilities.

The best way of conducting a comprehensive test would be to involve both internal and external tests. The internal perspective resembles the situation where attacks come from inside of the organisation´s safety perimeter, for example, insider attacks, whereas the external perspective resembles outside attacks. However, resources are often limited, and full, comprehensive tests cannot be conducted. [14, pp.109-112] In this test, the external perspective is used, as the idea is to simulate real communication situation, and test its information security. However, this thesis also includes internal test results from ThereGate, as it was selected as a target in an automation system security auditing course at TUT Department of Automation Science and Engineering.

6.2.1 Target and layout

This test will concentrate on public interfaces, as they are the most vulnerable parts of the system. However, wireless technologies such as Z-Wave and WLAN are left out of the scope. The idea of the testing is to simulate a real communication situation, and analyse the information security of that system. The goal of information security is to secure the confidentiality, integrity and availability of the system. Figure 6.1 presents what kind of system the testing simulates, and also which interfaces are to be tested.

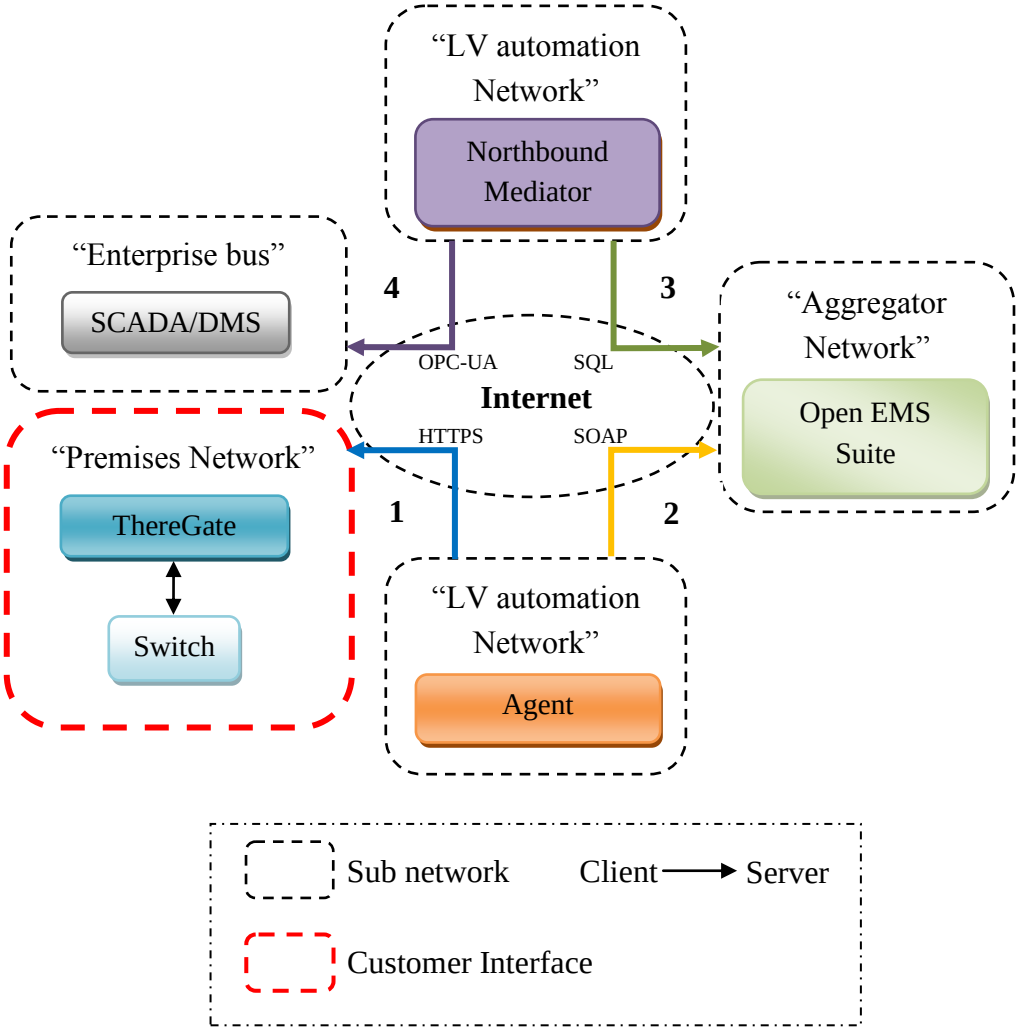

***Figure 6.1**. Simulated testing environment with interfaces.*

As presented in the conclusion of the analysis, ThereGate and the interface between ThereGate and the Agent are the two most important parts of the system in every scenario. Thus, the main concentration of testing will be at ThereGate and in HTTPS.

6.2.2 Used tools

The tools presented here, are used in the actual testing part. These tools have been selected for their suitability and popularity. Other tools can also be used for similar purposes. [1, pp. 114-130; 84] All, except, Codenomicon´s Defensics, are free of charges to personal usage.

For port scanning, and mapping the network structure, software called Nmap version 5.59 beta 1 is used. Nmap uses raw IP packets to identify hosts, services, the OS, and other characteristics. The command line format for running Nmap is following:

```
nmap [Scan Type(s)] [Options] <host or net #1...[#N]>
```

Nmap also provides a graphical interface called Zenmap, which provides easier way of using the tool, and visualization of results. Both software can be downloaded from http://nmap.org. [85.]

For monitoring and saving network traffic, Tcpdump version 4.1.1 and Wireshark version 1.6.4 is used: Tcpdump is used to capture the traffic and Wireshark to analyze it. Using this combination is rather efficient, as Wireshark has more restrictions in capturing traffic than Tcpdump, but on the other hand, with Wireshark, it is much easier to analyze the traffic. Tcpdump can be downloaded from www.tcpdump.org, and Wireshark from www.wireshark.org. [86:87.]

For vulnerability scanning, Tenable Nessus version 4.4.1, and Nexpose version 5.0.3 are used. These tools are network vulnerability scanners that can identify hosts currently connected on the network, and any vulnerable services or applications that are running. Nessus scans were done on the auditing class. Nessus is free of charges to personal usage only (HomeFeed), and can be downloaded from www.tenable.com. Nexpose´s Community Edition is free of charge, and can be downloaded from http://www.rapid7.com/vulnerability-scanner.jsp. [31; 88.]

Nessus scanner includes a number of plugins for web application scanning, testing vulnerabilities like SQL injection, XSS, HTTP header injection, directory traversal, remote file inclusion, and command execution. However, as web applications are complex and unique, automated vulnerability scanners cannot reveal all vulnerabilities, thus also missing some of the critical ones. [89.] This limitation needs to be taken into account, and other solutions need to be used to provide enough testing coverage. One tool for testing web interfaces is w3af. W3af is open-source, and can be downloaded from http://w3af.sourceforge.net/. [90.]

For the penetrating test, software called Metasploit Framework 4.2.0 and Armitage version 11.22.11 are used. These tools continue where vulnerability scanning ends by trying to exploit known vulnerabilities to attack the target system. The Armitage is a type of UI and management software for Metasploit. Armitage can be downloaded freely from http://www.fastandeasyhacking.com/. Metasploit offers a community edition free of charges with less functionality, and slower update circles for exploits than the licensed versions. Metasploit can be downloaded from www.metasploit.com. [91;92]

Other software used for attacking against the system is Ettercap version 0.7.4- Lazarus. This software is used especially for conducting MITM attacks on local area network. Ettercap includes sniffing live connections, content filtering on the fly, and many other features. Ettercap can be downloaded for free from http://ettercap.sourceforge.net/. [93]

For fuzz testing, Codenomicon Defensics test platform is used. This tool is meant for robustness testing, and to find flaws from protocols. It sends fuzzed information to the test target, and tries to find flaws. The tool itself consists of many other tools, and a large variety of protocol test suites are available. The two fuzzer software are Traffic Capture Fuzzer, and Universal Fuzzer. The Traffic Capture Fuzzer analyzes the traffic,

and creates a test model based on that information, whereas Universal Fuzzer test cases are generated from sample template files. Neither of the tools requires protocol specification. More information of Codenomicon and their software can be found at www.codenomicon.com [94].

All tools, except for Codenomicon´s Defensics, are already preinstalled in BackTrack 5 tool collection. However, some updating is required in order to use the latest versions of these software. The BackTrack can be downloaded free of charge from www.backtrack-linux.org [95]. The following bullet list and Figure 6.2 represent how the used tools work on different layers of the OSI model.

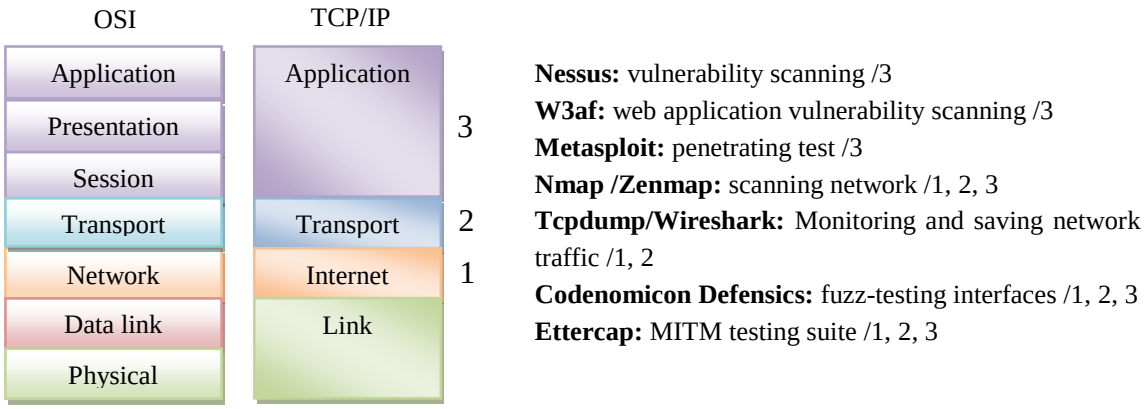

Figure 6.2. *Illustration of used software in different level of layers.*

As can be seen, the testing tools cover the different layers of the OSI model rather well. This is important in order to have a more comprehensive picture of the information security of the system.

6.2.3 Testing methodology

There are several testing methodologies to follow, each taking a bit of a different route. However, from each major methodology, a general approach can be found. This approach can be divided into four phases, which are: reconnaissance, discovery, vulnerability identification, and penetration [14, pp. 112-119].

This testing is done more in the spirit of white-box testing than black-box testing, as the tester knows IP addresses of the computers and such. Thus, the reconnaissance phase can be left to less attention. In this case, a more suitable approach for testing is the Homeland Security´s Hands-on Control Systems Cyber Security Training process, where the testing process is divided into four steps [96]:

1. Network Discovery
2. Vulnerability Analysis
3. Network Traffic Analysis
4. Network Exploitation

These four steps are also used in the testing phase, although in a different order. The following sub chapters describe in more detail what each of these steps includes.

Step 1. Network Discovery – Nmap

The first things to do, when auditing information security of any system, is to get information of which services and ports are open. From this information, it is easy to compare which ports should be open, and which ports really are open. It is also an important part of the awareness of how the system works, and what it consists of.

Step 2. Vulnerability Analysis – Nessus, Nexpose, w3af and Defensics

One significant factor in information security is to be aware of the versions of software used in the system. Especially the old versions are subject to vulnerabilities, which makes keeping software up-to-date important. Vulnerability scans can reveal not only the versions of the software and their vulnerabilities, but also other very important things, such as weak cipher supports, DoS vulnerabilities and so forth. Knowing which ports are open, and which OS is used really helps to select right plugins to the vulnerability scan. Not only does it speed up the process, but it can also have an impact on the scan as well.

There are also vulnerabilities in protocols. As the communication protocols are the cornerstone of the communication, it is important to know their vulnerabilities and test them, in order to gain a more comprehensive test coverage.

Step 3. Network Traffic Analysis – Tcpdump and Wireshark

In order to really know what information using which protocol is going to whom in the system, it is necessary to capture traffic, and analyze it. This is also an important part of fuzz-testing, as it requires a deeper understanding of protocols, and example sequences of protocols. Another important thing that can be discovered from the captured traffic is how the protocols have been done; for example, how the sequences change.

Step 4. Network Exploitation – Ettercap and Metasploit with Armitage

The results of the vulnerability scan can be used to exploit the vulnerability, and to try and penetrate the system under test. This part of the testing can require a deeper knowledge of programming, but there are also automated exploits that do not require much of an understanding.

Successful penetration of the system works as an example visualizing the fact that that information security issues are not irrelevant, or cannot be exploited. This is practical especially when trying to make the decision makers understand the importance of information security. [14, p. 110.]

6.2.4 Execution of testing

The actual testing is done in two parts. In the first series of testing, the equipment is scanned with Nmap, Nessus and w3af to find known vulnerabilities. This information is then used with Metasploit to attack each computer, one at a time. The second testing series concentrate in using Codenomicon´s Defensics and Ettercap against the interfaces of the system. In both parts, Tcpdump and Wireshark are used to monitor and analyze the traffic. Especially in the second part, Wireshark is used to get the right kind of data information to Defensics. Figure 6.3 below presents the actual testing configuration layout.

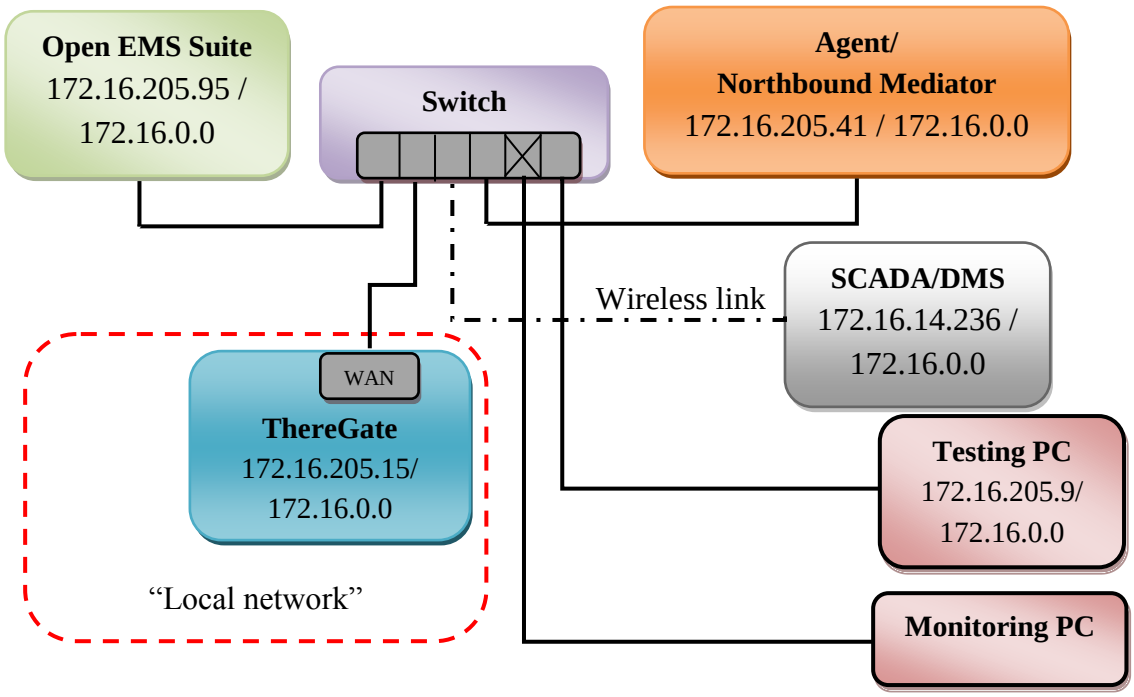

Figure 6.3. *The layout of the actual testing.*

As can be noticed, the testing is done using only one testing computer and one monitoring computer. All devices are connected to each other with a switch. As ICS is located in a different room, a wireless link is used to connect it to the system. Another noticeable thing is that Agent and Northbound Mediator are located in the same computer.

6.3 Testing results

The following test results have been gained by using the previously presented four step testing methodology. During the testing, the system was working normally. In this case, this means that the information from ThereGate went through the system, ending up to the ICS. However, as during the testing ThereGate´s GUI or SSH, for instance, were not used, they are not included in normal traffic in this case.

ThereGate is one of the most important equipment of the system, as it is the customer interface to the system. As a part of an auditing course (ACI-31070 Advanced Course in Network Based Automation, Fall 2012: Automation system auditing) of TUT, ThereGate was analyzed more closely by one group (participants Mikko Salmenperä, Marko Seppälä, and Kim Paananen). Some of the material of this information security auditing that was not revealed in the white box-testing is presented here. ThereGate was chosen for target because it was considered to be the most vulnerable, and at the same time, a crucial part of Smart Grid.

As the penetration testing with Metasploit did not result in penetration of any of the computers, it has been left out of the results. The Nmap and Nessus scan results for each computer are represented in appendix A. The results from other tools used are presented in the text.

6.3.1 Open ports and services

Interfaces are connection points to the system; they are used for communication with other computers and systems. Behind every interface is software, a service, which is using transmission control protocol/user datagram protocol (TCP/UDP) ports for communication. These interfaces are also the ones that adversaries use to attack against the system; they are trying to find vulnerability of interface, and exploit that to penetrate the system. It is especially the remotely accessible network services that are under serious threats. Common flaws, like poor configuration of web servers, mail servers, file and print servers, and DNS servers installed by default, often without a need for the given service, are the paths that the adversaries use. Additionally, many software automatically install services turning them on as part of installation, without any word to the administrator. These excess services that are not used in normal activity of the system only enlarge the attack surface, and possess vulnerabilities that adversaries may exploit to penetrate the system. [97.]

Findings from the testing

According to Nmap scan, there are four open ports in ThereGate. However, closer analysis of the captured traffic with WireShark reveals that only TCP port number 443 is used, when the system is working normally. As no SSH connections were used in the testing, TCP port number 22 was not used. However, there are two HTTP servers that are listening to different ports: Apache on TCP port 443 and CherryPy on TCP port 8080. The idea behind using two servers in this environment is that only one of the servers is communicating to outside of the system. This indicates that there is some sort of a configuration flaw in ThereGate´s software.

Other interesting port found by Nmap scan is the TCP port number 53. This port is used by the DNS server, over which a TCP wrapper service is working. This service can be used to deny or allow access to various services on the machine using access list rules [98]. TCP wrappers are actually a very important part of Unix´s information secu-

rity. However, the access list must be done properly. DNS server, if not needed, should be disabled, or restrict the access to internal hosts only, if the service is available externally.

The Nmap scan result from OES shows that there are 12 TCP, and four UDP ports open in the OES. Most of the services running in these ports are necessary for the system. However, from the analysis of the captured traffic, it can be seen that only a few ports are used during normal communication with other components: TCP ports number 8080 and 1521. These ports are the connection points to the Agent and Northbound Mediator. As no SSH connections were used in the testing, TCP port number 22 was not used. This means that there might be some ports open for no good reason. For example, TCP port number 9100 is used by a service called *jetdirect*, which is a printing service. This port might be used, for example, to steal sensitive information, thus having an impact on the confidentiality [99]. Other interesting ports and services, which are necessary to check, include SSH service in port 22, and HTTP servers in port 80 and 8086.

The list of open ports in the ICS computer is rather long, while there is only one port used during normal communication with other components; TCP port number 4850. This port is used between the connection with Northbound and the ICS. What is interesting about this is that Nmap scan or other vulnerability scanners did not reveal the port number 4850 at all. This indicates that some sort of firewall or other restricting feature is used in the ICS.

The rather numerous listing of open ports is due to the fact that in a normal running environment, ICS is a part of TUT´s domain and office network. However, it can be clearly seen that some hardening has already taken place in the ICS computer. Nevertheless, these open ports should be dealt with, one by one, making sure that each of them has a needed function in the system.

The Agent/Northbound (later Client) computer includes the client sides of the interfaces, meaning that there should not be too many open ports. Only the connection between the Agent and OES, which uses SOAP, requires that both ends include server and client sides. There are, however, some ports open, the purpose of which is not clear from the information communication point of view: HTTP service in port 5357, and *apj13* service in port 8009.

Probably the most interesting part of the Client computer analysis is the traffic analysis, as it includes all the client sides of the interfaces. During normal usage of the system, the Agent has connections to ThereGate´s port number 433, and OES´s port number 8080, whereas Northbound has connections to OES´s port number 1521, and ICS´s port number 4850. Table 6.1 presents the connections that are the core of the communication system of the testing environment.

The TCP port number of client side usually changes over time. In SOAP communication, each party has both server and client side, taking turns in which is the sending and which the receiving party. The one that is sending always has port number 8080. This has been illustrated in the table by showing that both ends of the interface have the same port number.

Table 6.1. *The interfaces of the system with IPs, ports and names.*

Server	IP	Port		Client	IP	Port
ThereGate	172.16.205.15	443	<-	Agent	172.16.205.41	many
OES	172.16.205.95	8080	<->	Agent	172.16.205.41	8080
OES	172.16.205.95	1521	<-	Northbound	172.16.205.41	many
ICS	172.16.14.236	4850	<-	Northbound	172.16.205.41	many

Table 6.2. *Overall TCP traffic of the system from the analysis.*

Destination PC	Destination port	Percent of TCP traffic
OES	9402	73 %
ICS	3389	16 %
ThereGate	443	3 %
ICS	4850	3 %
OES	8080	2 %
OES	1521	1 %

The analysis of the captured traffic, however, reveals that the system uses other ports and servers as well. Table 6.2 above presents the data flow from clients to servers. As it can be seen, 89% of the Client TCP traffic is something else than core communication traffic (highlighted with colour red). However, further analysis indicates that the TCP port 3389 is used for remote host terminal connection between the ICS and Client computer. For this reason, there are several ports open in both ICS and Client computers. In the real environment, however, this connection does not exist.

Another unknown open port, 9402, is used by IBM WebSphere Application Server for Common Secure Interoperability Version 2 (CSIv2), which is an authentication protocol. CSIv2 is implemented in WebSphere Application Server, and is used for implementing security features. [100.] According to the traffic capture, the parties of this connection are OES Server CA0, and OES User CA0. This connection is used by OES UI, which is used from the Client computer. WebSphere, and especially the application server, have numerable vulnerabilities, the most common being the DoS vulnerabilities [101; 102]. As OES is built on this software, these vulnerabilities can have a severe impact on the whole system.

Remediation

Every entity should make a baseline of what services and ports should be open. Network scanners, like Nmap, can be used to discover services provided to the inside and outside of the networks. These scans should be done regularly, and against the baseline. Especially any server that is visible from a public network, like the Internet, should be verified. Services that are not essential for business should be removed. Critical services, like DNS, file, mail, web, and database servers should be operated on separate physical host machines. Applying host-based firewall or port filtering tools, with a de-

fault deny-rule to all traffic, except that explicitly allowed, is essential. If unauthorized traffic or service is noticed, it should be blocked, and an alarm generated. [97.]

6.3.2 Version of software

One significant factor of information security is to be aware of the versions of software used in the system. Adversaries are constantly scanning an organization´s network looking for vulnerable versions of software. Especially old versions are subject to vulnerabilities that are well-known, and against which there are automated exploits to use. Adversaries also use web content, for instance, files, documents, pictures and so on, to attack and compromise target machines with malware, exploiting client side software vulnerabilities, like flaws in the browser. [97.]

Findings from the testing

According to the Nessus scan report, four high, and two medium severity problems come from a used hypertext preprocessor (PHP) 5.3 version, whereas one high, and four medium security problems comes from a used Apache 2.2 version. Each of these problems holds in them multiple vulnerabilities, which, if exploited, may result in different ways from DoS to full penetration of the system. There are also other software that use the old version. For example, ThereGate uses mod_ssl version 2.2.15, which is vulnerable to a remote buffer overflow, possibly leading to allowing a remote shell (CVE-2002-0082 and OSVDB-756). Outdated software is not so uncommon in embedded equipment, but nevertheless possesses great vulnerabilities.

Obviously, the servers of the OES have been configured more precisely, and are more up-to-date than those of ThereGate´s, for according to the Nessus´s report, there is only one high severity problem in the OES. However, there are problems that are due to the used version of software. For example, the installed version of Mort Bay Jetty is prone to multiple XSS vulnerabilities, which can, for instance, be used for stealing one´s identity, thus having an impact on confidentiality. Also the used version of Apache is prone for DoS.

With Nessus scan, it is also clear that the ICS computer has been hardened. There are only one high, and two medium severity problems that Nessus can find. The biggest problem, it seems, is vulnerability in Microsoft SQL Server that could allow remote code execution (CVE-2008-5416). Successful exploitation could allow an attacker to take complete control of the system. Also, used version of the remote desktop protocol server is vulnerable to a MITM attack.

The result from Nessus scan reveals that there is not a single high severity problem in the Agent computer. There are, however, seven medium severity problems, six out of seven of which are due to the old version of Apache Tomcat. These problems hold in them multiple vulnerabilities, such as XSS and DoS.

Remediation

To protect the system against these types of attacks, it is essential to keep the software up-to-date and patched. Especially for the software that has to do with a public network, such as the Internet, it is important to install security updates as soon they are released. Being a part of a software development society and email lists can also give a heads up, and more time to patch one´s software. In order to gain better protection, it is also essential that the end users are using secure client software. Informing customers how to make, for example, browsers more secure is a good practice, and should be presented, for instance, on a company´s website. [103.]

6.3.3 Software configuration

The way software has been configured has a huge impact on the information security of the entire system. Default configurations are often insecure and concentrated more on the easiness of use and deployment. Adversaries are also aware of the default setting and other most common configuration flaws, and are constantly searching for such software. These flaws are highways for adversaries to the system. [97]

Findings from the testing

The configuration problems of ThereGate are much more than just giving out information about the equipment. At the current status of ThereGate, due to the configuration flaws, it would be extremely easy for an adversary to penetrate the system. For example, configurations of PHP and Apache server have been done extremely wrong, enabling the adversary to penetrate the system simply using the browser. Of course, one has to remember that ThereGate is equipment under development, and many things will be changed in the commercial version. However, some of the flaws only make the development much harder, and also, it is more likely that some of the flaws remain, and end up in the commercial version. The following examples present some of the configuration flaws found from ThereGate (usernames and passwords have been changed).

Only one user - root

```
root:$1$YyZk36/l$xAVSoPxiMnc0dc4125LFI/:0:0:root:/tmp:/bin/
bash
nobody:*:65534:65534:nobody:/var:/bin/false
messagebus:!:10:10:messagebus:/var:/bin/bash
```

Apache configuration flaw

```
<Directory />
  Options FollowSymLinks
  AllowOverride None
  Order deny,allow
  Allow from all
</Directory>
```

PHP configuration flaw

```
root@TG-0000003:~# cat
sess_71e56950ad368b005365a9fe0678e576
user-
name|s:5:"admininistrator";password|s:11:"qwerty1234";error
|N;success|N;
```

As can be seen, there are many flaws in the configurations of ThereGate. Other flaws not presented here include directory enumeration, password auto complete, and so forth. These flaws can be used to gain complete access to ThereGate, violating all goals of the CIA.

Remediation

The basic things to do are to change default passwords as soon as possible, and delete example files from the server. However, it is necessary that before installing any software, especially a server, to familiarize yourself with articles on common configuration flaws, and best practice lists. Avoiding most common flaws, and configuring the server according to best practice gives an excellent starting point to make a baseline that can be used to monitor changes.

6.3.4 Information disclosure

Information disclosure, a situation where systems make information, such as details of installed software available to an outside person, is a rather common flaw of many systems. Although it may seem harmless, this vulnerability is, in fact, a serious flaw, since finding out, for example, the version of Apache helps the adversary to find the right, well-known vulnerabilities to exploit, in order to attack against the system. [104.]

Findings from the tested computers

From each of the computers, remote services with their version numbers can be detected. For example, ICS Microsoft SQL server version is 9.0.2039.0, hosted in port 1104. However, compared to ThereGate and the OES, the ICS and Agent are not revealing that much information.

OES, for its part, reveals a great deal of information, giving out, for example, names and versions of http Jetty server, IBM WebSphere Application Server, and remote transparent network substrate (TNS) listener. Each of these components has well-known vulnerabilities, giving, again, one excellent starting point for an adversary. For example, Oracle TNS protocol can fail to properly validate an authentication request, and Jetty HTTP server could allow a remote attacker to gain access to files outside the normal document tree [105; 106; 107].

From the Nmap and w3af scan results, it can be seen that ThereGate reveals too much information, giving out the names and versions of SSH, HTTP and SSL servers.

The scan also reveals the name and version of the OS, giving the adversary a great starting point. The error messages also reveal an awful lot of information, as presented in Figure 6.4 below.

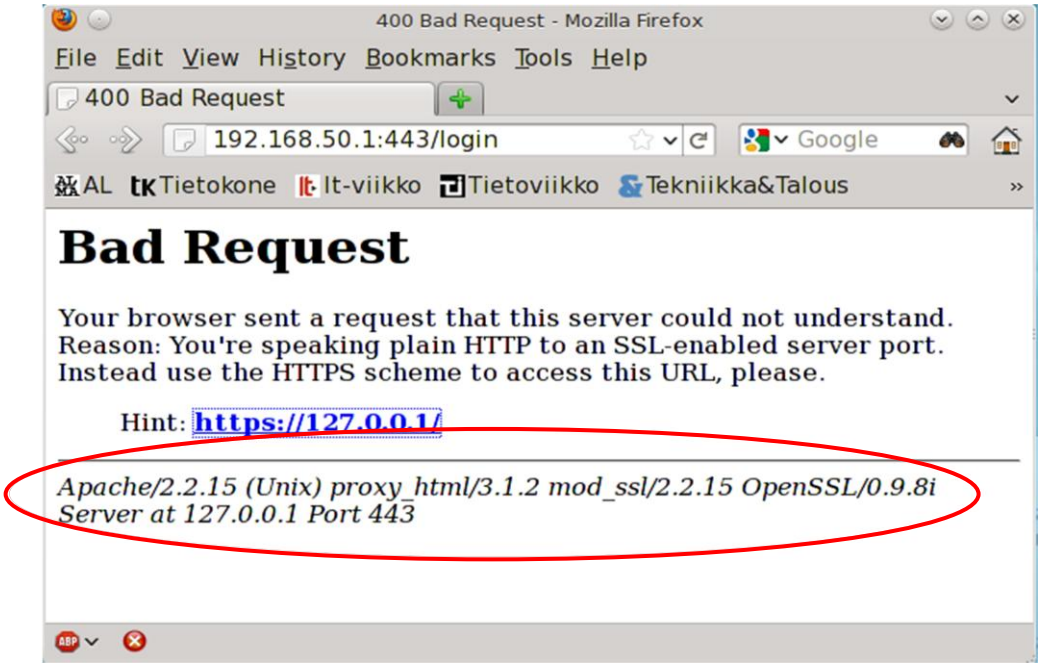

Figure 6.4. *'Bad Request'- message from ThereGate revealing too much information.*

As can be seen, the error message is rather informative, and reveals sensitive information. There are also other information disclosure issues, such as Easter Eggs, and the Internet control message protocol (ICMP) timestamp response. For example, from https://172.16.205.15/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000, some sensitive information can be seen.

Remediation

To protect the server from revealing too much information, one must configure the server right. Hiding the server number and other sensitive information is a matter of configuration, for example in Apache:

`ServerSignature Off` and `ServerTokens Prod`

However, security should not only rely on hiding things, but concentrate also on other solutions, like restricting access to a certain server, allowing only specific IPs. Other things that are often left to servers are the so called *Easter eggs*. While most of them reveal only funny pictures, some reveal sensitive information about the server. These Easter eggs, and other information disclosure features should be disabled. For example, setting 'expose_php' to 'Off' in PHP configuration file, – php.ini – disables

one information disclosure feature. Controlling the error messages is also a very important issue. Using a generic error message that does not reveal too much information is a good practice. [97; 18.]

6.3.5 Protocol flaws

One important part of any ICT system is communication protocols. Although many of these protocols, for instance, TCP or IP, have been used for a long time, they still have vulnerabilities. There are also newer protocols, and more seldom used protocols possibly possessing yet unknown vulnerabilities. As these protocols are the foundation of communication, and used by software and application, the vulnerabilities of these protocols can be severe. One of the easiest ways to exploit protocol flaws is to create some sort of a DoS attack, thus mostly impacting the availability. There are, however, more dangerous threats that these vulnerabilities possess, like allowing MITM types of attacks.

There are many vulnerabilities in protocols, and in how they, for example, establish connection. For example, the TCP connection-establishment mechanism could be used to perform a DoS attack by sending a large number of connection requests to the target system. This attack is also known as “SYN flood”, and it prevents the target system from establishing connections with legitimate users. Another type of an attack against TCP is hijacking the connection. To do this, the attacker must learn the sequence number from the ongoing communication, and forge a false segment that looks like the next segment. [108] IP protocol, too, has vulnerabilities; for example, IP spoofing, where adversary creates IP packets with a forged source IP address, in order to conceal the identity of the sender, or impersonate someone else. [107; 109.]

Computers communicate with each other via Ethernet (MAC) addresses. Address resolution protocol (ARP) is a mechanism that matches IP addresses with the addresses in an Ethernet network. This is done with broadcast messages that are sent to every computer. ARP poisoning is a MITM type of attack that exploits the ARP mechanism. ARP attacks, which can allow taking control of the packet flow, can be combined to TCP hijacking attacks in order to get permanent control of the hijacked TCP connection. [107; 110.]

Findings from the testing

One of the most relevant TCP ports of ThereGate is port number 433 that is used by both Agent and the GUI, and port number 22 that is used for SSH connection. The protocols that are communicating using port number 433 are TCP, HTTP and TLS. However, there are also other lower level protocols that are being used in the communication including ARP, ICMP, and IP protocols. All these protocols are ones that fuzz-testing concentrates on. The results from Codenomicon Defensics fuzzer software are represented in Table 6.3.

Table 6.3. *The results of ThereGate´s interfaces from Defensics.*

Protocol	ARP	ICMP	**IPv4**	**TCP**	HTTP	TLS	SSH
Port	-	-	**-**	**443**	443	443	22
Verdict	Pass	Pass	Fail	Fail	Pass/fail	Pass	Pass

Table 6.4. *The results of OES´s interfaces from Defensics.*

Protocol	ARP	**IPv4**	**TCP**	HTTP	SOAP	TNS
Port	-	**-**	**8080**	8080	8080	1521
Verdict	Pass	Fail	Fail	Pass/fail	Pass	Pass

As can be noticed, the higher level protocols did rather well in the test. Two protocols, however, did fail, those being IPv4 and TCP. In order to make the results more accurate, same tests were performed several times. Also, Defensics make it possible to run only the failed test cases, which speeds testing a lot. In the table, these have been presented in the *verdict* section with the following logic: if all tests were passed, the verdict is *pass*, if any of the tests were failed, the verdict is *fail*. If the result changed with the same test, the verdict is *pass/fail*. For example, HTTP passed the majority of tests, but failed two times with the same payload used. However, when the same payload and tests were done again, HTTP passed. Maybe in order to fail, HTTP needed some other impulse from, for example, the Agent, and, together with testing traffic resulted in failure.

The protocols that communicate using TCP port number 8080 are TCP, HTTP, and SOAP, whereas the protocols using TCP port number 1521 are TCP, and TNS. Other open ports, like 22, used by SSH, were left out of the scope. Table 6.4 above presents which protocols were tested, which port they used, and the verdict of the test result.

Just like with ThereGate, the only protocols to fail in fuzz-testing were IPv4, and TCP. HTTP protocol also behaved in a similar manner: in the first runs, it did not fail, but on the tests run second, it failed. The TNS protocol was tested using Traffic Capture software, as there were no ready test suites to that protocol. SOAP was also tested using this, as well as the SOAP test suite software. The Traffic Capture cannot provide as vast a testing coverage as protocol Test Suites, but nevertheless, gives at least some results. As OES is a high level part of the Smart Grid demonstration environment, a successful DoS attack would have a large impact on the availability of the entire system.

As there is only one interesting port - port 4850 – the fuzz-testing concentrates on this port. The OPC-UA TCP protocol was tested using Traffic Capture software, as there were no ready test suites to that protocol. Table 6.5 presents which protocols were tested, which port they used, and the verdict of the test result.

Table 6.5. *The results of ICS´s interfaces from Defensics.*

Protocol	**ARP**	**IPv4**	OPC-UA TCP
Port	-	**-**	4850
Verdict	Fail	Fail	Pass

Unlike any other component, ICS is the only one to fail the ARP protocol test. The used OPC-UA TCP implementation in the demonstration environment has been developed in TUT, and follows that specification [111]. Testing of OPC-UA TCP was rather hard due to the long handshake of the protocol. Nevertheless, the implementation seems to be rather solid.

However, some issues were found in the OPC-UA TCP implementation when analyzing the traffic. For example; the sequences start from zero, enabling the adversary to count what will be the next sequence, and possibility to perform a connection hijacking attack. Another found vulnerability is that if data is sent in several packages, the OPC-UA Server waits until it receives the last package. This can be used for DoS attacks.

Because of the limited resources, client side testing of interfaces was left out of the scope. It should, nevertheless, be mentioned that client side testing should also be performed in order to gain better testing coverage.

Remediation

To protect the system against protocol flaws may seem hard, if not even impossible. However, there are many ways to protect, or at least to diminish the impact and threat of these vulnerabilities. For example, against ARP poisoning, static ARP can be used where IP to MAC mappings are done manually. There are also surveillance tools, such as Arpwatch or Snort, which can be used to monitor unusual behaviour in the network. However, the most important thing is to design and implement the system correctly. Restricting what kind of information is allowed to a certain port is one example of improving the security. [109.]

6.3.6 Encryption of information

The thing that the adversaries are after, the asset, in the digital world, is information. As almost any ICT system of today consists of several components communicating with each other, it means that sensitive information needs to be transferred via communication lines. If this information is transferred in plain-text, it is extremely easy for adversaries to eavesdrop this traffic, resulting in data loss. This information could be used, for example, to impersonate a person or equipment, and gain authorized access to the system. In order to protect the transmission, encryption is used. However, not all encryption methods are that strong, and are prone for vulnerabilities. These vulnerabilities are well-known, and constantly searched by adversaries.

Findings from the testing

The already known fact, that is, the fact that encryption is used only between ThereGate and the Agent, was confirmed with analysis of the traffic. Encryption could, nevertheless, be used between all connections.

One of the most important parts of ThereGate and the whole demonstration environment is the web application interface, used by GUI and Agent. For this reason, HTTPS is also a crucial part of the system. As the older versions of TLS and SSL have well-known vulnerabilities, it is recommendable to use the newest ones. However, in the current version of ThereGate, SSL 2.0 is supported, as well as weak cipher suites. SSL 2.0 has well-known vulnerabilities and should not be supported at all. All in all, according to Nessus´s report, vulnerabilities in SSL cause four medium severity problems, and a few low severity problems as well.

One of the most recent vulnerabilities of SSL is the renegotiation issue [63]. This vulnerability was tested with special software created for this purpose only, thc-ssl-dos [112]. The result of the test indicates that renegotiations of SSL has been disabled, thus making the attack unsuccessful.

Remediation

To protect information, secure transmission protocols should be used. Even better is to use secure protocols that work in different layers at the same time, using, for example, IPSec and TLS. It is also essential to use strong versions of these secure protocols, and disable the support of old vulnerable versions, like SSL version 2.0. One way to check if the system is supporting weak SSL version 2.0, is to use simple command line testing, for instance:

`openssl s_client -connect` *`target`*`:`*`port`* `-ssl2 -cipher 'LOW:NULL:aNULL:EXPORT'` [113, pp. 34-35].

However, the key is in the planning process. The solution needs to take into account the long life span of software and equipment, and provide means to update encryption mechanisms to meet the standards of that time.

6.3.7 Authentication

Authentication is an essential part of any system, especially web applications. Knowing that the parties are who they claim to be is important, as otherwise no trust can be attained. There are, however, vulnerabilities in used authentication methods and procedures; for example, poorly designed application or login forms. Adversaries use brute force attacks, phishing email, MITM attacks, and many other attacks to learn credentials, or to bypass the authentication, as it is much easier than hacking into the system. If an adversary is authenticated falsely to the system, it can have devastating consequences.

Findings from the testing

The already known fact that there is some sort of client authentication between every component, except between Northbound and ICS, was verified with closer analysis of the traffic. The result unveils that the credentials used in authentication of clients are not that secure, and are subject to brute force attacks. As no encryption was used in these connections, the analysis of the credentials was rather straightforward.

Between ThereGate and the Agent, however, the situation is a bit different. It is typical that only the server is authenticated in HTTPS transactions, just like in this case, opening it to MITM attacks. In many situations, server authentication is enough, as it is only important to secure that the server is who it claims to be. In the Smart Grid environment, however, it is crucial to authenticate the client too. This means that HTTPS client must have a personal certificate in order to authenticate themselves. Usually these certificates must be signed by a CA, which is trusted by the server. In the demonstration environment, however, the client side authentication is done by using simple username/password authentication, and the server side certificates are not issued by a trusted CA. These create a false feeling of security and can have an impact on the confidentiality, and integrity of the system. In the commercial version of ThereGate, a certificate like X.509 is most likely used.

With software called Ettercap, different types of MITM attacks are possible to conduct [114]. The result from MITM attack between ThereGate and the Agent is most exciting, as it was the only one to use encryption. The result of this attack is presented below (username and password has been changed):

```
HTTP : 172.16.205.15:443 -> USER: administrator PASS:
qwerty1234 INFO: 172.16.205.15/api/login?username=
adminstrator&password=qwerty1234
```

As can be seen, Ettercap was successful in breaking SSL, and as a result, username and password are gained in plain-text. This is due to the fact that the client accepted the invalid certificate, which Ettercap provided. This is one example why self-signed, expired, or otherwise problematic certificates can be serious threats to the system.

Remediation

It is important to use secure transmission protocols, like HTTPS, when transmitting credentials, or other sensitive information. Planning and implementing the authentication procedure correctly is also essential. For example, by using HTTP POST and TYPE=PASSWORD in transmission. Using client side authentication as well improves the security of the system, as it is harder to conduct MITM attacks or impersonate someone. The widely used username - password combination, however, has been proved to be vulnerable, and does not alone provide sufficient security for more sensitive information. A more secure option is two-factor authentication, where user must provide something he or she knows, like username-password combination, and some-

thing he or she owns, like hardware token, mobile phone or biometrics for instance [115]. However, even this solution has its problems [116.]

Client certificates should only be used when needed, as they have their own problems, like the management of the certificates. If used, they should be supported with hardware, like a TPM. The recent events of hacked CAs do not help the situation either, as the number of trustworthy entities has decreased [117]. As the reliability of the CAs has shaken, other more secure solutions need to be planned and used. In the demonstration environment, a simple public key infrastructure (SPKI) type of solution could work better, as there is no need for commercial CAs.

6.3.8 Other found issues

As mentioned in the previous chapter five, embedded systems most often have computational constraints. ThereGate is no exception. When ThereGate was under Nessus external network vulnerability scan or Ettercap DoS attack, it crashed several times, rebooting the whole machine. Thus, ThereGate, with its current hardware, is prone to DoS type of attacks, having an impact on the availability of the system. The solution to this problem is to use white and black lists in firewalls or other traffic limitations, and ensure that the programs used in ThereGate are optimised.

The other tests that measured protocols were done with Ettercap, which turned out to be a very powerful tool. The DoS attack of Ettercap was used against each component of the system, resulting in different levels of DoS.

6.3.9 Synopsis of the test results

Each interface can be divided into components that it consists of. These are the most critical parts of the interfaces, and of the whole system, and the ones that must be protected. For example, HTTPS interface includes TCP/IP, HTTP and TLS protocols, and of course, a server and a client. The server, for one part, consists of configurations, used programming language and so forth.

In order to make the results more compact and understandable, they can be divided into three groups:

1. Configuration flaws
2. Software flaws
3. Implementation flaws

Table 6.6 presents the most critical flaws divided into three groups for each interface. To be said, this table does not include all flaws found, just the most critical ones.

Table 6.6. *Summary of test results divided into groups.*

Target	**Configuration flaw**	**Software flaw**	**Implementation flaw**
ThereGate: -HTTP -TCP/IP - TLS -Apache -PHP	CherryPy listens port 8080. Reveals too much information (SSL, SSH, HTTP Servers). Only one user – root. Apache: *allow from all.* PHP: session management: user id in plaintext. TSL weak cipher & version support. Easter Eggs	Apache version 2.2 vulnerabilities. PHP version 5.3 vulnerabilities. SSL version	No client auhentication. No CA certifications. IP and TCP protocols fail. HTTP protocol failure. Computational constrains, DoS ARP poisoning
OES: -HTTP -TCP/IP - Jetty - WebShpere - Apache	Unnecessary services and open ports: *jetdirect, ...* Too many services are visible. Reveals too much information (HTTP, WebShpere, TNS). LDAP NULL BASE Search Access. Web Server prone to HTML injections, XSS attacks.	Apache Byte Range DoS. Mort Bay Jetty Multiple XSS . WebSphere.	IP and TCP protocols fail. HTTP protocol failure. No CA certifications. No encryption Weak client authentication ARP poisoning
ICS: - ARP - TCP/IP - SQL Server	Too many services are visible. Microsoft Windows SMB Null Session Authentication.	Microsoft SQL Server: remote code execution.	ARP and IP protocols fail. OPC-UA TCP issues No encryption No authentication ARP poisoning
Agent: - TCP/IP - Apache	Unnecessary services and open ports: *apj13, ...* Too many services are visible. Apache Tomcat contains example files. Web Server uses plain text authentication forms.	Apache Tomcat 7.x vulnerabilities.	ARP poisoning

As can be seen, configurations are extremely important, being able to make a good system insecure, and vice versa. With good configuration and a firewall, it is possible to create a good level of security, and manage vulnerabilities that cannot be fixed by, for example, hiding them. Another very important factor is to keep the software updated and patched. The milestones of the whole ICT system are communication protocols. If they fail, so will the applications using them.

7 BEST PRACTICES SECURITY CHECK LIST

This chapter sums up the obtained results in the form of a best practices security check list that can be used for evaluating information security of a home automation system. Finding an apt solution for information security can be hard, but on the other hand, companies working in Smart Grid cannot afford to ignore it.

Automation systems just like Smart Grid are utilizing ICTs. Thus, the best information security practices for the Smart Grid follow closely those of a normal ICT environment. However, every situation is unique, and possesses characteristic features that affect what can be done and what cannot. For example, updating software and OS in automation environment can be impossible. The key for securing any system is to know the goals – what are the objectives of information security – and its targets – what are the assets of the system that needs to be protected. When these two have been determined, it is easier to identify the most critical parts of the system.

In order to keep the whole process under control, the system should be divided into smaller pieces, segments and go systemically through each component, one at a time. Also, once a good configuration, for example, to switch has been made, it can be applied to other switches and make it into an organization´s security policy.

7.1 Customer Domain – HEMS/Home automation:

A crucial part of HEMS security is the customers' awareness, and how well their computers are secured. Companies should try to provide at least some sort of a best practices checklist for the end users to follow. Also, companies should concentrate more on default settings, and realize the laziness of human beings; default passwords, for instance, are not always changed. One could say that the three most critical software to secure a user's computer are a firewall, virus scanner, and correct configuring of the web browser. Whereas the firewall and virus scanners are familiar to most of the people, browser settings are not. Plug-ins, like Flash, make things even more complicated. Yet, it is commonly known that most of the Internet attacks of today exploit the client side software vulnerabilities [67].

According to CERT-FI, it is necessary for an active Internet user to save one´s registration information. This information includes the address of the site, username, password (not to be located in computers hard-drive, or encrypted), email address, and information if a credit card has been used or not. This way, when sites are penetrated, one can easily see what information has been compromised and so forth. [103.] However, when conducting a list including all your information and passwords, the issue is where

to keep it. There are tools for managing passwords that could be one solution for managing the information.

This checklist is designed for companies and entities that are providing home automation related services or equipment like ThereGate in customer domain. Working in this domain is probably the most challenging from the information security point of view as there are many interconnection points and most of all, as public interfaces are often needed. Also, the competition in this domain is hard leaving very little resources to information security aspects.

The equipment are most often used by normal people. For this reason, this checklist also tries to take into account the special features that the variety of people brings along. Following best practice security checklist has been made from the findings of this thesis as well as using many other best practices lists.

Critical control 1: Physical security

The purpose of this control

Physical interfaces are among the easiest of ways to bypass other security features that the equipment might have. According to studies made, two-thirds of all USB memory sticks can infected with malware! [118]. As the home automation devices will be at the customer´s domain, and used by customers as well, devices with external physical ports, such as USB ports, will have to face this problem.

How to implement

Companies making home automation devices should think which features they want to offer, and then think how they can make it safe. There are different ways of approaching physical safety. For example, using seals is one way to prevent, or at least prove that the equipment has been used incorrectly. Other solutions try to monitor which devices are connected, or restrict how and what it is possible to do via physical ports. One way to shrink the time window of a possible attack is to force a company´s own firmware once a day.

How to test

Below it is presented how to check, which interfaces or devices are used in the system. Additionally, by using software such as arpwatch, it is possible to monitor unknown mac-ip pairs that have been connected to the system [119].

- In Windows: *devcon listclass usb* or *wmic cpi list brief*
- In Linux: *lsusd* or *dmesg | tail*

Critical control 2: Limitation of services and open ports

The purpose of this control

Unnecessary open ports and provided services are serious threats to any system – to Smart Grid too. Limiting the number of available services and open ports decreases the attack surface of the system, making it more compact, and easier to defend. Especially DNS, file and print servers, SSH and such, need to have good reasons for why they are enabled [97]. No server should be provided in the spirit that it might be used at some point. As OSs, like Windows, and a great number of other software open many unnecessary ports and services as a default installation, this control needs to be done to every system. As a side result of this control, deeper understanding, and a state of awareness of the system is gained.

How to implement

To perform this control there are many different routes to follow. OSs have integrated features, like netstat, that can be used to monitor which ports are open, and what services are provided. There are also software, like Nmap, that can be used to scan the system from inside and from outside to monitor, and learn what things are visible to network [85]. It is important to make a baseline and use these tools frequently to compare the results against the baseline.

How to test

A few commands from the above mentioned tools are presented below.

- In Windows: *netstat –a* or *netstat –r* or *netstat –a –n | findstr LISTENIGN*
- In Linux: *lsof –in* or *ps-al* or *netstat*
- With Nmap: *nmap –p 1-65535 –T4 –A –v <IP>*

Critical control 3: Up-to-date software

The purpose of this control

Using up-to-date software is almost a truism in a normal ICT environment of today. However, in a traditional automation system, where updates are not installed frequently, and where old OSs are still used, using updated software is rarer. In a home automation environment, where public Internet is a part of the architecture, and new techniques are used, installing security updates as soon as they are release is a critical factor. Thus, updating circles are faster too, and it is important to design the system to be flexible in this matter.

How to implement

There are many ways to monitor, which versions of software are used in the computer. OSs, as well as external software, provide means to do that.

How to test
A few ways of finding out information about software are presented below.

- About Windows OS: *C:\>systeminfo | findstr /C:"OS"*
- About Linux OS: *cat /proc/version* and *cat /etc/banner*
- About PHP (linux): */usr/bin/php-cgi --version*
- Nmap and Nessus scans

Critical control 4: Secure default configuration and installation

The purpose of this control
Home automation devices and software will be at customer domain and most often also used by normal people. So far, the default settings of these kinds of commercial devices and software have been concentrating on the easiness of use and deploy rather than security. However, most of the people do not change default settings, like passwords, making these devices and software easy targets for adversaries.

How to implement
Instead of focusing solely in the easiness of installation and implementation, companies should concentrate also to the security of default settings and installation process. For example, forcing to change default passwords to ones strong enough in installation process is one way to improve security. Companies must recognise and understand the nature of people, and take responsibility of the information security of the equipment.

Critical control 5: Two-way authentication

The purpose of this control
With authenticating both ends of communication, better security is provided. Ensuring that both parties of communication are who they say to be, is crucial, especially in environment where better security is required, like Smart Grid environment. [120; 121.] Given the recent development, it is probable that smart phones will also be used in Smart Grid environment. This creates more challenges to design and deploy secure authentication process. Authenticating only server side makes the connection more prone to attacks such as MITM and pharming. These attacks if successful could have devastating consequences to whole Smart Grid.

How to implement
Basically, secure client side authentication requires the use of digital signatures and a certificate issuance scheme, or two-factor authentication for individual user level authentication [120]. Using commercial CAs is not always the best solution given the recent events of hacked CAs. Better solution for home automation environment could be using SPKI, for instance. In web based authentication SSL should always be used and

HTTP basic should be replaced with HTTP digestive. Also, the authentication process must be done easy enough to adopt and maintenance, so that it will not be bypassed.

- Support client certificates with hardware, like TPM
- In forms:
  - Use always HTTP POST when transmitting credentials
  - Use 'TYPE=PASSWORD'
- Allow only strong enough passwords
  - Passwords absolute minimum length is nine character
  - Passwords have special characters, upper, and lower case letter and numbers
- Limit the usage of same password with expiration policy
- Limit the number of subsequent unsuccessful authentication tries, for example
  - After ten times, lock the username for half an hour

Critical control 6: Secure session management

The purpose of this control

One of the most common vulnerabilities of web-based systems is insecure session management [122, p 2]. Vulnerabilities in this process are most often serious as they can allow adversary to steal sensitive information, like sessionID and impersonate user. Using encryption is important and gives more security, but cannot fix all problems: vulnerabilities in session management can traverse encryption [122, p 25]. As automation equipment can provide web UI for customers to manage the equipment, for instance, this control is applicable for many companies in Smart Grid environment.

How to implement

There are different methods that can be used for session management. Each of these methods can be made reasonable secure with intelligent design. But on the other hand, with negligence and incompetence each can be insecure [122, p 4]. One of the most important things in secure session management is the management of sessionID. Choosing a long enough, 256 bits, and random sessionID protects the system against brute force attacks, for instance [123]. Using best practise security list gives excellent starting point and helps avoiding most common mistakes.

- Make sure that the sessionID is random and long enough, 256 bits
- Check that the sessionID changes with every login
- Check that sessionID desolates when logout
- Make sure that no user information can be derived from sessionID
- Use strong encryption on all transmissions
- Store only the Session ID on the Client Side
- Perform sanity checks to detect session hijacking

Critical control 7: Secure communication encryption

The purpose of this control

One of the easiest ways for the adversary to learn something about the system is eavesdropping, if no encryption is used. SSL is an industry, and de facto standard for establishing an encrypted link between client and server. However, there are vulnerabilities even in SSL as well as and in other encryption methods, which adversaries exploit to attack against the system. Most commonly, these attacks result in DoS types of situations, but other more severe situations are also possible. In Smart Grid environment, there is plenty of sensitive information that needs to be transmitted in an encrypted form. If information is transmitted, for example, from meters to HEMS in plain text, it is very easy to spoof.

How to implement

The milestone in securing that the encryption used is strong enough, is to disable the support of old versions, and making sure that only high level encryption versions are used. To improve security even more, different levels of security features, such as IPSec and TLS, should be used.

How to test

Presented below is a simple way to check if a weak version of SSL is supported by the system:

- Using command: *openssl s_client -connect target:port -ssl2 –cipher 'LOW:NULL:aNULL:EXPORT'* [113, pp. 34-35].

Critical control 8: Secure software configuration

The purpose of this control

Software configurations are an essential part of any system´s information security. In a home automation environment, especially configuring web servers needs to be done with the utmost care. One example of the importance of configuration is information disclosure: giving out detailed information about the system may help an adversary to find vulnerabilities from the system. In a home automation environment, where information security is somewhat newer thing than in a normal ICT system, there might be more zero-day vulnerabilities. Information disclosure does not only apply to servers telling too much information about services, but also error messages and such. From a detailed error message, great deal of information can be attained.

How to implement

The basic things to do are to change the default passwords as soon as possible, and delete example files from the server. However, it is necessary that before installing any software, especially a server, to familiarize yourself with articles on common configura-

tion flaws and best practice lists. Avoiding most common flaws and configuring the server according to the best practice gives an excellent starting point to make a baseline, which can be used to monitor changes. [97.] Using vulnerability scanners like Nessus or w3af will also give hints of bad configurations. Presented below are a few basic things about configuring software:

- Use best practice lists to help setting the configurations of servers
  - Apache: http://www.petefreitag.com/item/505.cfm
  - PHP: http://www.cyberciti.biz/tips/php-security-best-practices-tutorial.html
- Change default passwords as soon as possible
- Delete example files from the server
- Delete other than necessary parts of the service
- Use generic error message that does not reveal too much information
- Make sure that the server runs with limited rights
  - Apply sandboxes
- Turn off directory browsing
  - Apache .htaccess file: *Option –indexes*
  - Especially cgi-bin

Critical control 9: Validate information

The purpose of this control

Home automation devices are part of Smart Grid, and many other services or operations may be relying on their information. Especially when altering such information could be profitable for customers, companies must ensure the integrity of information. If the information that comes from devices cannot be trusted, it will ultimately affect to entire Smart Grid.

Validating information is also very important way of improving a systems security. Without proper input validation, the adversary might gain access to "deeper" parts of the system, conducting attacks like SQL injections and such. This might lead, for instance, to loss of sensitive information. Validation of input is also a critical part of any web application of today for the reasons stated above.

How to implement

The key of validation of information is to check all information coming from users or equipment consists of only accepted characters. Applying white-lists is also one way to control the information.

- Check that all information coming from users/equipment consists only of accepted characters (including forms, http-headers, cookies and url-parametres)
- Use white lists

Critical control 10: Secure control of information

The purpose of this control

In many ICT systems, information needs to be kept in databases where it can be distributed to legal parties. The recent events of hacked web servers give excellent example of the importance of secure control of information. In home automation environment a lot of sensitive information is transferred and databases used. Vulnerabilities in this process may result in loss of sensitive information, for instance.

How to implement

The starting point of secure information control is to use always encryption when sensitive information is transmitted. Also, asking and storing only necessary information is a good starting point. Sensitive information, like passwords should not be kept in plaintext format, but instead use cryptographic hash functions, like MD5 or SHA1 and salt combined with a password. Taking safety backups from the database and keeping it in safe location, is also, good practise and helps to act in cases of database penetrations, for instance. One easy way to increase user security is to confirm all passwords management changes using, for example registered email address. [103.]

8 CONCLUSION

The two goals set to this thesis were to introduce a way to analyse and test information security of Smart Grid ICT implementation and to provide best practice security checklist for entities in the home automation environment. The results from the analysis and testing phase point out the necessity of information security analysis. As it turned out, each of the ICT equipment has information security issues, some more than others. The most common vulnerabilities came from software configuration and using vulnerable versions of software.

The most crucial equipment in the demonstration environment is ThereGate: it is the customer´s UI to the entire Smart Grid. However, the information security of ThereGate has serious shortages, which can be used to exploit the equipment. If the security of ThereGate is compromised, it will affect the whole system. Therefore, securing ThereGate should be priority number one. However, it should be noted that the used ThereGate is a development version and is therefore not intended for production. It is probable that some ISP or DSO will own ThereGate and, consequently is also responsible for securing it. However, in order to a gain good security level, companies must work together.

The best practice security checklist takes into account the special characteristics of the home automation environment in Smart Grid. The most important asset of the system is information, which makes protecting it the main goal. This requires better security methods, like two-way authentication or two-factor authentication as well as using secure encryption versions. However, companies working in the home automation environment also have to take into account the human factor and make sure that every costumer, regardless of her or his knowledge of technology, can securely use the services and equipment provided.

Smart Grid environment also needs stricter requirements from the used protocols and specifications. It is clear, that as long as standards and other only recommend, not require information security methods, like encryption and such, they will not be used and thus, make the system more vulnerable. Stricter policies and requirements are needed.

Smart Grid is a complex and a huge environment. This thesis only scratched the surface of this iceberg, concentrating in certain parts of it. It is clear that more studies on information security are required in order to create a secure Smart Grid.

REFERENCES

[1] Ahonen, P. TITAN – käsikirja. VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa. Espoo 2010. VTT Tiedotteita – Research Notes 2545. 152 p. In Finnish

[2] Stouffer, K, Falco, J, Scarfone, K. Guide to Industrial Control (ICS) Security. Recommendations of the National Institute of Standards and Technology. June 2011, special publication 800-82. 155 p. [PDF]. [Referred 8.12.2011]. Accessible from: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

[3] Imperva. Hacker Intelligence Initiative, Monthly Trend Report #5. Redwood City, California 2011. [PDF]. [Referred 12.12.2011]. Available from: http://www.imperva.com/docs/HII_Monitoring_Hacker_Forums.pdf.

[4] YouTube. [WWW/video]. [Referred 8.12.2011]. Accessible from: http://www.youtube.com/watch?v=6kfBXVhu-k0.

[5] Brown, F. Pulp Google Hacking. The next Generation Search Engine Hacking Arsenal. Hacker Halted, Miami 2011. [PDF]. [Referred 12.12.2011]. Available from: http://www.stachliu.com/slides/2011/Hacker%20Halted%202011%20-%20Pulp%20Google%20Hacking%20-%2027Oct2011.pdf.

[6] Cubrilovic, N. This is how Facebook tracks you. Betanews, 2011. [WWW]. [Referred 12.12.2011]. Available from: http://betanews.com/2011/09/26/this-is-how-facebook-tracks-you/.

[7] Hypponen, MH. Defending the Net. TEDxBrussels, 2011. [WWW/Video]. [Referred 1.12.2011]. Available from: http://www.tedxbrussels.eu/2011/speakers/mikko_h_hypponen.html.

[8] Kan, M. China Restricts Local Media From Sourcing Info From Internet. PCWorld, 2011. [WWW]. [Referred 1.1.2012] Available from: http://www.pcworld.com/article/243602/china_restricts_local_media_from_sourcing_info_from_internet.html.

[9] Brown, E. Renault tips Androud IVI system, seeks app developers. LinuxDevices.com, 2011. [WWW]. [Referred 12.12.2011]. Available from: http://www.linuxfordevices.com/c/a/News/Renault-RLink/?kc=rss.

[10] Seppälä, J. Tietoturva on osa automaation käytettävyyttä (Security is part of the automation dependability). Automaatioväylä 5/2008. pp. 9-11. In Finnish.

[11] Suomen automaatioseura ry. Teollisuusautomaation tietorurva (Information security of industry automation). Verkottumisen riskit ja niiden hallinta. 1st publication. Helsinki 2005. Painomerkki Oy. 160 p. In Finnish

[12] Grimvall G., Holmngren Å., Jacobsson P. & Thedéen T. Risks in Technological Systems. London 2009. Springer. 341 p.

[13] The Smart Grid Interoperability Panel – Cyber Security Working Group. Guidelines for Smart Grid Cyber Security vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. National Institute of Standards and Technology. 2010. 289 p. [PDF]. [Referred 2.8.2011]. Accessible from: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

[14] Flick, T., Morehouse, J. Securing the Smart Grid. Next Generation Power Grid Security. Burlington, USA, 2011. 290 p.

[15] Schneier B. Secrets & Lies: Digital Security in a Networked World. Indiana, Wiley, 2000. 414 p.

[16] Helmbrecht, U, Purser, S, Klejnstrup, M. Cyber security: future challenges and opportunities. Enisa, European network and information security agency. [PDF]. [Referred 1.10.2011]. Available from: www.enisa.europa.eu/publications /position-papers/cyber-security-future-challenges-and-opportunities/at_download/fullReport.

[17] Ahonen, P. Constructing network security monitoring systems (MOVERTI Deliverable V9). Espoo 2011. VTT tiedotteita – Research notes 2589. [PDF]. [Referred 1.12.2011]. Available from: http://www.vtt.fi/inf/pdf/tiedotteet/2011/T2589.pdf.

[18] TYPO3. TYPO3 Security Guide, version 1.0.0. [WWW]. [Referred 11.11.2011]. Available from: http://typo3.org/documentation/document-library/extension-manuals/doc_guide_security/1.0.0/view/.

[19] Microsoft – TechNet, Windows 2000 Server, Library. Common Types of Network Attacks. [WWW]. [Referred 25.9.2011]. Available form: http://technet.microsoft.com/en-us/library/cc959354.aspx.

[20] OWASP - The Open Web Application Security Project. Gategory: Vulnerability. [WWW]. [Referred 20.11.2011]. Available form: https://www.owasp.org/index.php/Category:Vulnerability.

[21] The Economist. War in the fifth domain. 7/2010. [WWW]. [Referred 2.8.2011]. Accessible from: http://www.economist.com/node/16478792.

[22] McMillian, R. Was Stuxnet Built to Attack Iran´s Nuclear Program? PCWorld, 9/2010. [WWW]. [Referred 5.12.2011]. Available form: http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

[23] BBC. News UK. News of the World phone-hacking scandal. 8/2011. [WWW]. [Referred 5.11.2011]. Available form: http://www.bbc.co.uk/news/uk-11195407.

[24] Kotilainen, S. Hakkerit: nyt veimme Sonyltä miljoonan käyttäjän tiedot. Tietokone 6/2011. In Finnish. [WWW]. [Referred 2.8.2011]. Available from: http://www.tietokone.fi/uutiset/hakkerit_nyt_veimme_sonylta_miljoonan_kayttajan_tiedot.

[25] Sapronov, K. The human factor and information security. Securelist 11/2005. [WWW]. [Referred 5.7.2011]. Available form: http://www.securelist.com/en/analysis/176195190/The_human_factor_and_information_security.

[26] Leighton, T. The Net´s Real Security Problem. Scientific American. 8/2006 [WWW]. [Referred 20.10.2011]. Available form: http://www.scientificamerican.com/article.cfm?id=the-nets-real-security-pr&colId=32&page=1.

[27] Navy & Marine Corps WWII Commemorative Committee. Navajo Code Talkers: World War II Fact Sheet. [WWW]. [Referred 20.11.2011]. Available form: http://www.history.navy.mil/faqs/faq61-2.htm.

[28] Deng, J. Introduction to Symmetric Block Cipher. University of Colorado, lecturing material. [PPT]. [Referred 1.12.2011]. Available from: www.cs.colorado.edu/~jrblack/class/csci7000/f03/talks/7000_1.ppt.

[29] Menezes, A, Van Oorschot P, and Vanstone, S. Handbook of Applied Cryptography. Chapter: Overview of Cryptography. 1996. 49 p. [PDF]. [Referred 1.12.2011]. Available from: http://www.cacr.math.uwaterloo.ca/hac/about/chap1.pdf.

[30] SNORT. Intrusion prevention and detection system developed by sourcefire. [WWW]. [Referred 19.9.2011]. Available from: http://www.snort.org/.

[31] Nessus. Vulnerability scanner developed by Tenable. [WWW]. [Referred 19.9.2011]. Available from: http://www.tenable.com/products/nessus.

[32] IPHE ILC meeting. The Utsira wind –hydrogen project. 2005. [PDF]. [Referred 2.8.2011]. Available from: http://www.iphe.net/docs/Meetings/Brazil_3-05/Norway_Utsira_Wind_H2.pdf.

[33] Green World Investor. Germany Solar Energy Market World´s Biggest. Green Subsidies fuel growth German Photovoltaic Panel, Cell, Inverter, Manufacturers. 3/2011. [WWW]. [Referred 2.12.2011]. Available from: http://www.greenworldinvestor.com/2011/03/19/germany-solar-energy-market-worlds-biggest-green-subsidies-fuel-growth-german-photovoltaic-panelcellinverter-manufacturers/.

[34] SGEM Unconference 2011. Siuntio, Finland 16-17.11.2011.

[35] NIST. Smart Grid Interoperability Standards Roadmap. Post Comment Period Version. 2009. 184 p. [PDF]. [Referred 2.8.2011]. Available from: http://www.nist.gov/smartgrid/upload/Report_to_NIST_August10_2.pdf.

[36] Renner, S, ALbu, M, Elburg, H, Heinemann, C, Lazicki, A, Penttinen L, Puente, F, Saele, H. European smart metering landscape report. Smart Regions deliverable 2.1. Vienna 2011. [WWW]. [Referred 14.11.2011]. Available from: http://www.smartregions.net/_ACC/_Components/ATLANTIS-DigiStore/Download.asp?fileID=253415&basketID=1522.

[37] Cottingham, J. South Korea – smart grid revolution. ZPryme. [PDF]. [Referred 2.1.2012] Available from: http://www.smartgridinformation.info/pdf/4560_doc_1.pdf.

[38] Lima, C. Enabling a Smarter Grid. Smart Grid Communications. Silicon Valley 2010. [PDF]. [Referred 16.10.2011] Available from: http://www.ewh.ieee.org/r6/scv/comsoc/Workshop_092510_EnablingSmarterGrid.pdf.

[39] Gunther, E, Snyder, A, Gilchrist, G, Highfill, D. Smart Grid Standards Assessment and Recommendations for Adoption and Development. EnerNex Corporation. 2/2009. [DOC]. [Referred 12.10.2011]. Available from: http://www.osgug.org/Shared%20Documents/Smart%20Grid%20Standards%20Landscape%20White%20Paper%20v0%2083.doc.

[40] ABB. Toward a smarter grid: ABB's vision for the Power System of the Future. [PDF]. [Referred 2.8.2011]. Available from: http://www02.abb.com/db/db0003/db002698.nsf/0/36cc9a21a024dc02c125761d0050b4fa/$file/Toward_a_smarter_grid_Jul+09.pdf.

[41] EurActiv. Smart Grids could save Europe €52bn. 11/2010. [WWW]. [Referred 2.9.2011]. Available from: http://www.euractiv.com/energy-efficiency/smart-grids-could-save-europe-52bn-news-499738.

[42] EU Comission Task Force for Smart Grids. Expert group 3: roles and responsibilities of actors involved in the smart grids deployment. 4/2011. [PDF]. [Referred 5.10.2011]. Available from: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group3.pdf.

[43] European SmartGrids – Technology platform. Vision and strategy for europe´s electricity networks of the future. Belgium 2006. 22 p. [PDF]. [Referred 19.9.2011]. Available from: http://www.smartgrids.eu/documents/vision.pdf.

[44] Wind energy – the facts. Grid infrastructure upgrade for large-scale integration. [WWW]. [Referred 17.10.2011]. Available from: http://www.wind-energy-the-facts.org/en/part-2-grid-integration/chapter-4-grid-infrastructure-upgrade-for-large-scale-integration/.

[45] Nordpool spot. How does it work. [WWW]. [Referred 3.10.2011]. Available from: http://nordpoolspot.com/How-does-it-work/.

[46] Nasdaq omx commodities. About NASDAQ OMX Commodities. [WWW]. [Referred 7.10.2011]. Available from http://www.nasdaqomxcommodities.com/about/.

[47] Eurelectric. Regulation for Smart Grids. 2011. 44 p. [PDF]. [Referred 8.10.2011]. Available from: http://www.eurelectric.org/Download/Download.aspx?DocumentFileID=66894.

[48] IEEE: the expertise to make smart grid a reality. Smart Grid Conceptual model. [WWW]. [Referred 14.10.2011]. Available from http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model.

[49] Office of the National Coordinator for Smart Grid Interoperability. NIST framework and roadmap for smart grid interoperability standards, realease 1.0. Special Publication 1108. 2010. 145 p. [PDF]. [Referred 23.9.2011]. Available from: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

[50] Conant, R. Towards a global smart grid – The U.S. vs. Europe. Trilliant. Electric light & power. [WWW]. [Referred 8.10.2011]. Available from: http://www.elp.com/index/display/article-display/2702271845/articles/utility-automation-engineering-td/volume-15/Issue_5/Features/Toward_a_Global_Smart_Grid_-_The_US_vs_Europe.html.

[51] Kerola, J. 22 000 sähkömittaria vaihtoon Tampereella oikosulkujen takia (22 000 smart meters changed in Tampere due the short circuit problem). Aamulehti, 6.10.2011. In Finnish. [WWW]. [Referred 8.10.2011]. Available from: http://www.aamulehti.fi/Pirkanmaa/1194699838443/artikkeli/22+000+sahkomittaria+vaihtoon+tampereella+oikosulkujen+takia.html.

[52] Zhang, Z. Smart Grid in America and Europe: similar desire, different approaches (part 1). 1.1.2011. [PDF]. [Referred 15.9.2011]. Available from: http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1799705_code1465129.pdf?abstractid=1799705&mirid=1.

[53] Koto A., Lu S., Rautiainen A., Repo S. & Valavaara T. Demonstration environment for smart grid applications. Tampere University of Technology - Department of Electrical Energy Engineering. The second version, 2011. 40 p. [PDF]. [Referred 1.9.2011]. Available from: http://webhotel2.tut.fi/units/set/research/inca-public/tiedostot/Raportit/OES_ThereGate_demo.pdf.

[54] Hardesty, L. The too-smart-for-its-own-good grid. MIT 3.8.2011. [WWW]. [Referred 14.9.2011]. Available from: http://web.mit.edu/press/2011/too-smart-grid.html.

[55] Nokia Siemens Network. Common interests, common platform. Open EMS Suite gets the industry talking. 10/2007. [PDF]. [Referred 5.9.2011]. Available from: http://www.nokiasiemensnetworks.com/system/files/document/Open_EMS_Suite_Brochure.pdf.

[56] There Corporation. ThereGate. [WWW/PDF]. [Referred 9.9.2011]. Available from: http://www.therecorporation.com/en.

[57] Burns S. Threat Modeling: A Process To Ensure Application Security. SANS Institute InfoSec Reading Room, 2005. 13 p. [PDF]. [Referred 3.8.2011]. Available from: http://www.sans.org/reading_room/whitepapers/securecode/threat-modeling-process-ensure-application-security_1646.

[58] Ambler S. Agile Modeling – Introduction to Security Threat Modeling. [WWW]. [Referred 3.8.2011]. Available from: http://www.agilemodeling.com/artifacts/securityThreatModel.htm.

[59] Liikenne- ja viestintäministeriö. Laajakaista kaikkien ulottuville. Kansallinen toimintasuunnitelma tietoyhteiskunnan infrastruktuurin parantamiseksi. (Broadband for everyone to reach. National action plan to better the infrastructure of information society). In Finnish. [WWW]. [Referred 3.8.2011]. Available from: http://www.lvm.fi/web/fi/viestinta/strategiat/strategia/-/view/1127095.

[60] Arvinen, M. Etäluettavat sähkömittarit tulevat kaikkiin koteihin (smart meters are coming to every households). 7.3.2011. [WWW]. [Referred 15.11.2011]. Available from: http://www.sahkoala.fi/koti/lehti/suunnittelu/fi_FI/etaluettavat_sahkomittarit/_print/.

[61] HomePNA. Existing Wires Home Networking. [WWW]. [Referred 23.11.2011]. Available from: http://www.homepna.org/.

[62] CERT. CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks. 29.11.2000. [WWW]. [Referred 25.11.2011]. Available from: http://www.cert.org/advisories/CA-1996-21.html.

[63] Perry, D. New DoS Tool Kills SSL Servers With Just One PC. Tom´s hardware, 26.10.2011. [WWW]. [Referred 26.11.2011]. Available from: http://www.tomshardware.com/news/security-attack-DOS-SSL-server-email,13818.html.

[64] Trusted Computing Group. Trusted Platform Module. [WWW]. [Referred 16.10.2011]. Available from: http://www.trustedcomputinggroup.org/developers/trusted_platform_module/.

[65] Microsoft. Mikä on TPM (trusted platform module) – turvapiiri? (What is TPM module?). In Finnish. [WWW]. [Referred 2.9.2011]. Available from: http://windows.microsoft.com/fi-FI/windows-vista/What-is-the-Trusted-Platform-Module-security-hardware.

[66] eNotes – study smarter. Cold boot attack. [WWW]. [Referred 30.10.2011]. Available from: http://www.enotes.com/topic/Cold_boot_attack.

[67] SANS. The Top Cyber Security Risks. 9/2009. [WWW]. [Referred 15.11.2011]. Available from: http://www.sans.org/top-cyber-security-risks/.

[68] Schneier, B. 2006 Operating System Vulnerability Study. 2.4.2007. [WWW]. [Referred 18.11.2011]. Available from: http://www.schneier.com/blog/archives/2007/04/2006_operating.html.

[69] Christey, S. 2011 CWE/SANS Top 25 Most Dangerous Software Errors. Common Weakness Eumeration 7/2011. [WWW]. [Referred 15.11.2011]. Available from: http://cwe.mitre.org/top25/index.html#CWE-89.

[70] Z-Wave World. Forums – general discussion – Z-Wave products and technology. 2007. [WWW]. [Referred 23.10.2011]. Available from: http://zwaveworld.com/forum/lofiversion/index.php?t133.html.

[71] Z-Wave. Products that speak Z-Wave together better. [WWW]. [Referred 23.10.2011]. Available from: http://www.z-wave.com/modules/Products/?id=38&chk=9da4368a23a117f445aa61f4f93c265e.

[72] Lane, H. Security Vilnerabilites and Wireless LAN Technology. SANS Institute InfoSec Reading Room. Virginia Beach, 2004. 18 p. [PDF]. [Referred 23.10.2011]. Available from: http://www.sans.org/reading_room/whitepapers/wireless/security-vulnerabilities-wireless-lan-technology_1629.

[73] Wexler, J. WPA2 Vulnerability Found. PCWorld – Security, 25.7.2010. [WWW]. [Referred 25.10.2011]. Available from: http://www.pcworld.com/article/201822/wpa2_vulnerability_found.html.

[74] Educated Guesswork. Understanding the TLS Renegotiation Attack. 5.11.2009. [WWW]. [Referred 25.10.2011]. Available from: http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html.

[75] InfosecStuff. TLS Vulnerability. Putting the TLS Vulnerability Into Perspective. 9.11.2009. [WWW]. [Referred 27.10.2011]. Available from: http://www.infosecstuff.com/?tag=tls-vulnerability.

[76] US-Cert. Vulnerability Note VU#945216. SSH CRC32 attack detection code contains remote integer overflow. [WWW]. [Referred 5.11.2011]. Available from: http://www.kb.cert.org/vuls/id/945216.

[77] Bhalla, N, Kazerooni, S. Web Services Vulnerabilities. A white paper outlining the application-level threats to web services. 15.2.2007. 12 p. [PDF]. [Referred 8.11.2011]. Available from: http://www.blackhat.com/presentations/bh-europe-07/Bhalla-Kazerooni/Whitepaper/bh-eu-07-bhalla-WP.pdf.

[78] Layer 7 technologies. White Paper: XML Threats and Web Services Vulnerabilities: Understanding Risk and Protection. 2005. 8 p. [PDF]. [Referred 13.11.2011]. Available from: http://www.soahub.com/Architecture/PDF/XML_Threats_Web_Services_Vulnerabilities.pdf.

[79] Peterson, D. OPC DA Articles. OPC UA: Specification Vulnerabilities. 26.1.2010. [WWW]. [Referred 5.11.2011]. Available from: http://opcda.info/index-sel-articles-id-21.htm.

[80] Yle. Suojaamattoman WLAN-yhteyden salakäyttö halutaan sallia (The use of unprotected WLAN wanted to be permitted). 24.1.2011. In Finnish. [WWW]. [Referred 16.11.2011]. Available from: http://yle.fi/alueet/perameri/2011/01/suojaamattoman_wlan-yhteyden_salakaytto_halutaan_sallia_2288958.html.

[81] Elisa Oyj. Viihde. In Finnish. [WWW]. [Referred 16.11.2011]. Available from: http://www.elisa.fi/viihde/.

[82] McLaughlin, Sm Podkuiko, D, McDaniel, P. Energy Theft in the Advanced Metering Infrastructure. Systems and Internet Infrastructure Security Laboratory. Pensylvenia State University. 12 p. [PDF]. [Referred 17.11.2011]. Available from: http://www.patrickmcdaniel.org/pubs/critis09.pdf.

[83] OWASP. OWASP Testing Guide, version 3.0. 2008. 349 p. [PDF]. [Referred 17.11.2011]. Available from: https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf.

[84] Sectools. SecTools.Org: Top 125 Network Security Tools. [WWW]. [Referred 19.11.2011]. Available from: http://sectools.org/.

[85] NMAP. Network discovery tool. [WWW]. [Referred 11.1.2012]. Available from: http://nmap.org/.

[86] Tcpdump. Traffic capture tool. [WWW]. [Referred 11.1.2012]. Available from: http://www.tcpdump.org/.

[87] Wireshark. Traffic capture and analyze tool. [WWW]. [Referred 11.1.2012]. Available from: http://www.wireshark.org/.

[88] NeXpose. Rapid 7. A vulnerability scanner. [WWW]. [Referred 11.1.2012]. Available from: http://www.rapid7.com/vulnerability-scanner.jsp.

[89] Martin, B, Fennelly, C. Web Application Scanning with Nessus. Detecting Web Application Vulnerabilities and Environmental Weaknesses. Revision 3, 2.9.2010. 14 p. [PDF]. [Referred 22.11.2011]. Available from: http://www.nessus.org/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/whitepapers/Tenable_Web_App_Scanning.pdf.

[90] W3af. Web Application Attack and Audit Framework. [WWW]. [Referred 11.1.2012]. Available from: http://w3af.sourceforge.net/.

[91] Metasploit. Open source community & Rapid7. Penetration test tool. [WWW]. [Referred 11.1.2012]. Available from: www.metasploit.com.

[92] Armitage. UI for Metasploit. [WWW]. [Referred 11.1.2012]. Available from: http://www.fastandeasyhacking.com/.

[93] Ettercap. MITM tool. [WWW]. [Referred 11.1.2012]. Available from: http://ettercap.sourceforge.net/.

[94] Codenomicon. Defensics, fuzzing tool. [WWW]. [Referred 19.11.2011]. Available from: http://www.codenomicon.com/defensics/.

[95] Backtrack 5. Collection of testing tools. [WWW]. [Referred 11.1.2012]. Available from: www.backtrack-linux.org.

[96] Homeland Security. Hands-on Control Systems Cyber Security Training. Course material. 184 p.

[97] SANS. 20 Critical Security Controls. Twenty Critical Security Controls for Effective Cyber Defence Consensus Audit Guidelines. [WWW]. [Referred 19.12.2011]. Available from: https://www.sans.org/critical-security-controls/.

[98] All about Linux. Using TCP Wrapper To Secure Linux. 8.8.2005. [WWW]. [Referred 23.12.2011]. Available from: http://linuxhelp.blogspot.com/2005/10/using-tcp-wrappers-to-secure-linux.html.

[99] Creenshaw, A. Hacking Network Printers. Irongeek. [WWW]. [Referred 23.12.2011]. Available from: http://www.irongeek.com/i.php?page=security/networkprinterhacking.

[100] IBM Education Assistant. IBM WebSphere Application Server V6. Security. Common Secure Interoperability Version 2. 8.6.2006. [WWW/Video]. [Referred 27.12.2011]. Available from: http://publib.boulder.ibm.com/infocenter/ieduasst/v1r1m0/index.jsp?topic=/com.ibm.iea.was_v6/was/6.0/Security/WASv6_Sec_CSIv2/player.html.

[101] Saint corporation. Vulnerability Tutorial – WebSphere vulnerabilities. 12.5.2011. [WWW]. [Referred 27.12.2011]. Available from: http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=WebSphere_vulnerabilities.html&fact_color=&tag.

[102] The Canadian Cyber Incident Response Centre. WebSphere Vulnerabilities. 7.3.2011. [WWW]. [Referred 2.1.2012]. Available from: http://www.publicsafety.gc.ca/prg/em/ccirc/2011/AV11-021-eng.aspx.

[103] CERT-FI. Ohje 1/2011 Verkkopalvelun ohjelmistoalustan valinta ja palvelun turvallinen ylläpito (Guidline 1/2011: Choosing Web service software platform and safe maintenance of the service). 25.11.2011. [WWW]. [Referred 2.1.2012]. Available from: http://www.cert.fi/ohjeet/2011_23/ohje-1-2011.html.

[104] Microsoft. Information Disclosure. [WWW]. [Referred 2.1.2012]. Available from: http://msdn.microsoft.com/en-us/library/aa738441.aspx.

[105] Shulman, A. The Untold Tale of Database Communication Protocol Vulnerabilities. Redwood Shores, California. Imperva. 46 p. [PDF]. [Referred 4.1.2012]. Available from: http://www.imperva.com/resources/adc/pdfs/the_untold_tale_of_database_communication_protocol_vulnerabilities.pdf.

[106] US-Cert. Vulnerability Note VU#402580. Jetty HTTP server directory traversal vulnerability. [WWW]. [Referred 2.12.2011]. Available from: http://www.kb.cert.org/vuls/id/402580.

[107] Ocepek, S, Henrique, W. Oracle, Interrupted: Stealing Sessions and Credentials. Trustwave. 20.4.2010. 51 p. [PDF]. [Referred 17.12.2011]. Available from: https://www.trustwave.com/downloads/spiderlabs/Trustwave-SpiderLabs-Oracle-Interrupted-Henrique-and-Ocepek.pdf.

[108] IETF. Security Assesment of the Transmission Control Protocol (TCP). Draft, 25.7.2011. [WWW]. [Referred 22.12.2011]. Available from: http://tools.ietf.org/html/draft-ietf-tcpm-tcp-security-02#section-5.

[109] Chambers, C, Dolske, J & Iyer, J. TCP/IP Security. Department of Computer and Information Science, Ohio State University. Columbia. [WWW]. [Referred 15.12.2011]. Available from: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html.

[110] Beekey, M. ARP Vulnerabilites – Indefensible Local Network Attacks? Black Hat Briefings ’01. 51 p. [PPT]. [Referred 15.12.2011]. Available from: http://www.blackhat.com/presentations/bh-usa-01/MikeBeekey/bh-usa-01-Mike-Beekey.ppt.

[111] Mikko Salonen. OPC UA –tietoturvatoteutus java-ohjelmointikielellä. Master´s Thesis. 2009. Tampere University of Technology. Automation technology. 86 p. [PDF]. [Referred 15.12.2011]. Available from: http://ae.tut.fi/research/AIN/Publications/Salonen,%20Mikko%20-%20OPC-UA,%20jaeltava_rajoitettu.pdf.

[112] THC-SSL-DOS. SSL testing tool. [WWW]. [Referred 15.12.2011]. Available from: http://www.thc.org/thc-ssl-dos/.

[113] Davis, C. Auditing Networks, Perimeter, and Systems. SANS Course: Advanced Audit 507. 51 p. [DOC]. [Referred 15.12.2011]. Available from: http://kickofflife.com/Documents/2005%20SANS%20Advanced%20Auditing%20Course%20Notes.ver.04.doc.

[114] Ettercap. MITM testing tool. [WWW]. [Referred 15.12.2011]. Available from: http://ettercap.sourceforge.net/.

[115] Valente, E. Two-Factor Authentication: Can You Choose the Right One? SANS Institute InsoSec Reading Room. 21 p. [PDF]. [Referred 19.12.2011]. Available from: http://www.sans.org/reading_room/whitepapers/authentication/two-factor-authentication-choose-one_33093.

[116] Schneier, B. The Failure of Two-Factor Authentication. 15.3.2005. [WWW]. [Referred 15.12.2011]. Available from: http://www.schneier.com/blog/archives/2005/03/the_failure_of.html.

[117] Bright, P. Comodo hacker: I hacked DigiNotar too; other CAs breached. Ars technica – security. 9/2011. [WWW]. [Referred 15.12.2011]. Available from: http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars.

[118] Cyber Media. Most lost USB sticks carry malware: study. 14.12.2011. Sophps. Mumbai. [WWW]. [Referred 10.1.2012]. Available from: http://www.ciol.com/Security/Mobile-Security/News-Reports/Most-lost-USB-sticks-carry-malware-study/157783/0/.

[119] Network Research Group of the Information and Computing Sciences Division at Lawrence Berkeley National Laboratory . LBNL's Network Reaseach Group. Berkeley, California. Arpwatch. [WWW]. [Referred 10.1.2012]. Available from: http://ee.lbl.gov/.

[120] Curphey, M, Endler, D, Hau, W, Taylor, Smith, T, Russell, A, McKenna, G, Parke, R & McLaughlin, K. A Guide to Building Secure Web Applications. OWASP, 22.7.2002. [WWW]. [Referred 10.1.2012]. Available from: http://www.cgisecurity.com/owasp/html/ch06.html.

[121] Duncan, R. An Overwiev of Different Authentication Methods and Protocols. 23.10.2001. SANS Institute InfoSec Reading Room. 9 p. [PDF]. [Referred 10.1.2012]. Available from: http://www.sans.org/reading_room/whitepapers/authentication/overview-authentication-methods-protocols_118.

[122] OWASP. Session Management Cheat Sheet. 21.10.2011. [WWW]. [Referred 10.1.2012]. Available from: https://www.owasp.org/index.php/Session_Management_Cheat_Sheet.

[123] Murphey, L. Secure Session Management: Preventing Security Voids in Web Applications. 10.1.2005. SANS Institute InfoSec Reading Room. 31 p. [PDF]. [Referred 10.1.2012]. Available from: http://www.sans.org/reading_room/whitepapers/webservers/secure-session-management-preventing-security-voids-web-applications_1594.

[124] Leeds, D. Who Are the Players in the Smart Grid and How Much is the Market Worth? 28.9.2010. Greentechgrid. [WWW]. [Referred 10.10.2011]. Available from: http://www.greentechmedia.com/articles/read/who-are-the-players-in-the-smart-grid-and-how-much-is-the-market-worth/.

APPENDIX A

Table A.1. *Nmap scan result of ThereGate.*

Port	Protocol	State	Service	Version
22	tcp	open	ssh	Dropbear sshd 0.52 (protocol 2.0)
53	tcp	open	tcpwrapped	
443	tcp	open	http	Apache httpd 2.2.15 ((Unix) proxy_html/3.1.2 mod_ssl/2.2.15 OpenSSL/0.9.8i)
8080	tcp	open	http	CherryPy httpd 3.1.2 (WSGI Server)

Table A.2. *Nmap scan result of OES.*

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
53	tcp	open	domain	
80	tcp	open	http	IBM HTTP Server (Derived from Apache)
111	tcp	open	rpcbind	2 (rpc #100000)
389	tcp	open	ldap	(Anonymous bind OK)
443	tcp	open	http	IBM HTTP Server (Derived from Apache)
1521	tcp	open	oracle-tns	Oracle TNS Listener 11.1.0.7.0 (for Linux)
8080	tcp	open	http	Jetty httpd 6.1.6
8086	tcp	open	http	Jetty httpd 6.1.15
9080	tcp	open	http	IBM WebSphere Application Server 6.1
9100	tcp	open	jetdirect	
9998	tcp	open	distinct32	
53	udp	open	domain	
111	udp	open	rpcbind	2 (rpc #100000)
123	udp	open	ntp	NTP v4
5353	udp	open	mdns	DNS-based service discovery

Table A.3. *Nmap scan result of ICS.*

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	
445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
1042	tcp	open	ms-sql-s	Microsoft SQL Server 2005 9.00.3042.00; SP2
1051	tcp	open	msrpc	Microsoft Windows RPC
1104	tcp	open	ms-sql-s	Microsoft SQL Server 2000 8.00.2039.00; SP4
1801	tcp	open	msmq	
2103	tcp	open	msrpc	Microsoft Windows RPC
2105	tcp	open	msrpc	Microsoft Windows RPC
2107	tcp	open	msrpc	Microsoft Windows RPC
2967	tcp	open	symantec-av	
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service
5555	tcp	open	remoting	MS .NET Remoting services
123	udp	open	ntp	Microsoft NTP
137	udp	open	netbios-ns	Microsoft Windows netbios-ssn (workgroup: FSIIPI)
1434	udp	open	ms-sql-m	Microsoft SQL Server 8.00.194 (ServerName: SCADA; TCPPort: 1104)

Table A.4. *Nmap Scan result of Agent/Northbound.*

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	
445	tcp	open	netbios-ssn	
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009	tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8080	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
49152	tcp	open	msrpc	Microsoft Windows RPC
49153	tcp	open	msrpc	Microsoft Windows RPC
49154	tcp	open	msrpc	Microsoft Windows RPC
49155	tcp	open	msrpc	Microsoft Windows RPC
49158	tcp	open	unknown	
49159	tcp	open	msrpc	Microsoft Windows RPC
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn (workgroup: SET)

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
55925	1	PHP 5.3 < 5.3.7 Multiple Vulnerabilities	High Severity problem(s) found
52717	1	PHP 5.3 < 5.3.6 Multiple Vulnerabilities	High Severity problem(s) found
51140	1	PHP 5.3 < 5.3.4 Multiple Vulnerabilities	High Severity problem(s) found
48245	1	PHP 5.3 < 5.3.3 Multiple Vulnerabilities	High Severity problem(s) found
55976	1	Apache HTTP Server Byte Range DoS	High Severity problem(s) found
26928	1	SSL Weak Cipher Suites Supported	Medium Severity problem(s) found
20007	1	SSL Version 2 (v2) Protocol Detection	Medium Severity problem(s) found
42873	1	SSL Medium Strength Cipher Suites Supported	Medium Severity problem(s) found
51192	1	SSL Certificate signed with an unknown Certificate Authority	Medium Severity problem(s) found
46803	1	PHP expose_php Information Disclosure	Medium Severity problem(s) found
51439	1	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	Medium Severity problem(s) found
44921	1	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	Medium Severity problem(s) found
11213	1	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) found
56216	1	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS	Medium Severity problem(s) found
53896	1	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Medium Severity problem(s) found
50070	1	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Medium Severity problem(s) found
48205	1	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Medium Severity problem(s) found

Figure A.1. *A part of Nessus scan report from ThereGate.*

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
55976	2	Apache HTTP Server Byte Range DoS	High Severity problem(s) found
51192	1	SSL Certificate signed with an unknown Certificate Authority	Medium Severity problem(s) found
44320	1	Mort Bay Jetty Multiple XSS	Medium Severity problem(s) found
12218	1	mDNS Detection	Medium Severity problem(s) found
10722	1	LDAP NULL BASE Search Access	Medium Severity problem(s) found
42797	1	Jetty CookieDump.java Sample Application Persistent XSS	Medium Severity problem(s) found
10595	1	DNS Server Zone Tranfer Information Disclosure (AXFR)	Medium Severity problem(s) found
49067	1	CGI Generic HTML Injections (quick test)	Medium Severity problem(s) found
47831	1	CGI Generic Cross-Site Scripting (comprehensive test)	Medium Severity problem(s) found
44136	1	CGI Generic Cookie Injection Scripting	Medium Severity problem(s) found

Figure A.2. A part *of Nessus scan report from OES.*

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
35635	1	MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) (uncredentialed check)	High Severity problem(s) found
26920	1	Microsoft Windows SMB NULL Session Authentication	Medium Severity problem(s) found
18405	1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium Severity problem(s) found

Figure A.3. *A part of Nessus scan report from ICS.*

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
12085	1	Apache Tomcat servlet/JSP container default files	Medium Severity problem(s) found
51976	1	Apache Tomcat 7.x < 7.0.6 Manager Interface Cross-Site Scripting	Medium Severity problem(s) found
55759	1	Apache Tomcat 7.x < 7.0.17 Multiple Vulnerabilities	Medium Severity problem(s) found
53323	1	Apache Tomcat 7.x < 7.0.12 Multiple Vulnerabilities	Medium Severity problem(s) found
52634	1	Apache Tomcat 7.x < 7.0.11 @ServletSecurity Annotation Security Bypass	Medium Severity problem(s) found
51526	1	Apache Tomcat 6.x < 6.0.30 / 7.x < 7.0.5 Multiple XSS	Medium Severity problem(s) found
51987	1	Apache Tomcat < 6.0.32 / 7.0.8 NIO Connector Denial of Service	Medium Severity problem(s) found

Figure A.4. *A part of Nessus scan report from Agent/Northbound.*

APPENDIX B

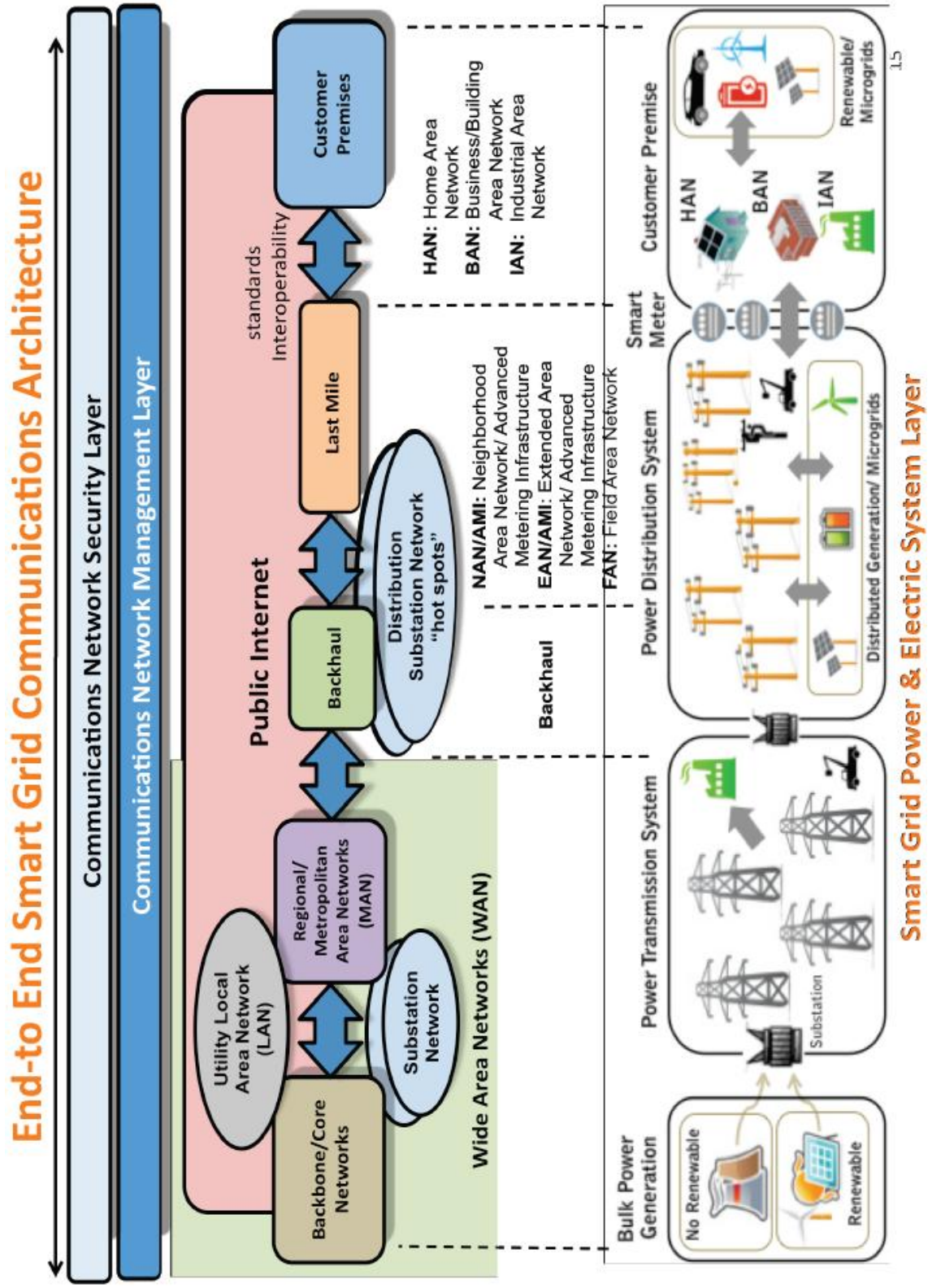

Figure B.1. *High level picture of communication and power layers [38].*

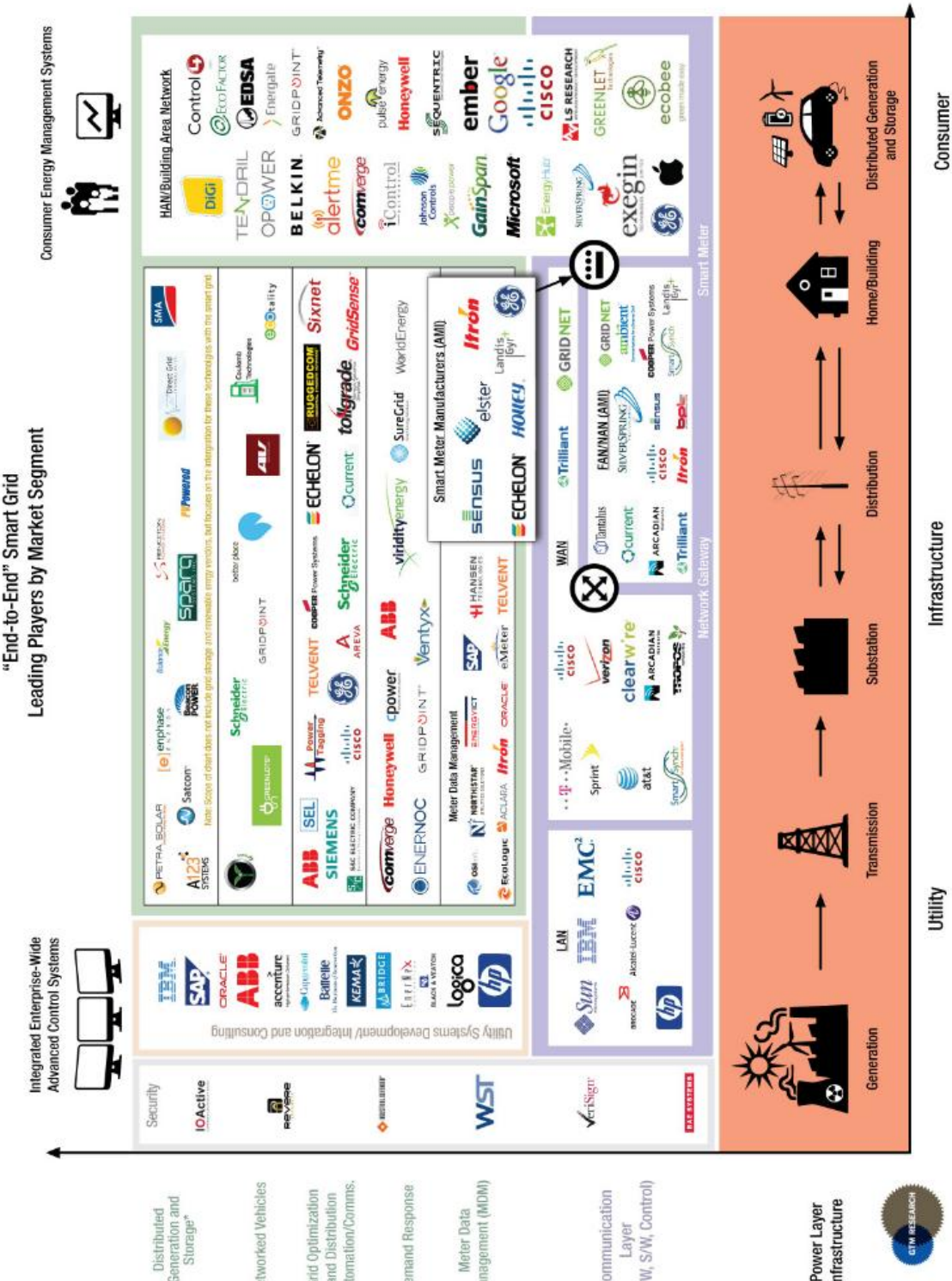

Figure B.2. *Players of the Smart Grid [124].*

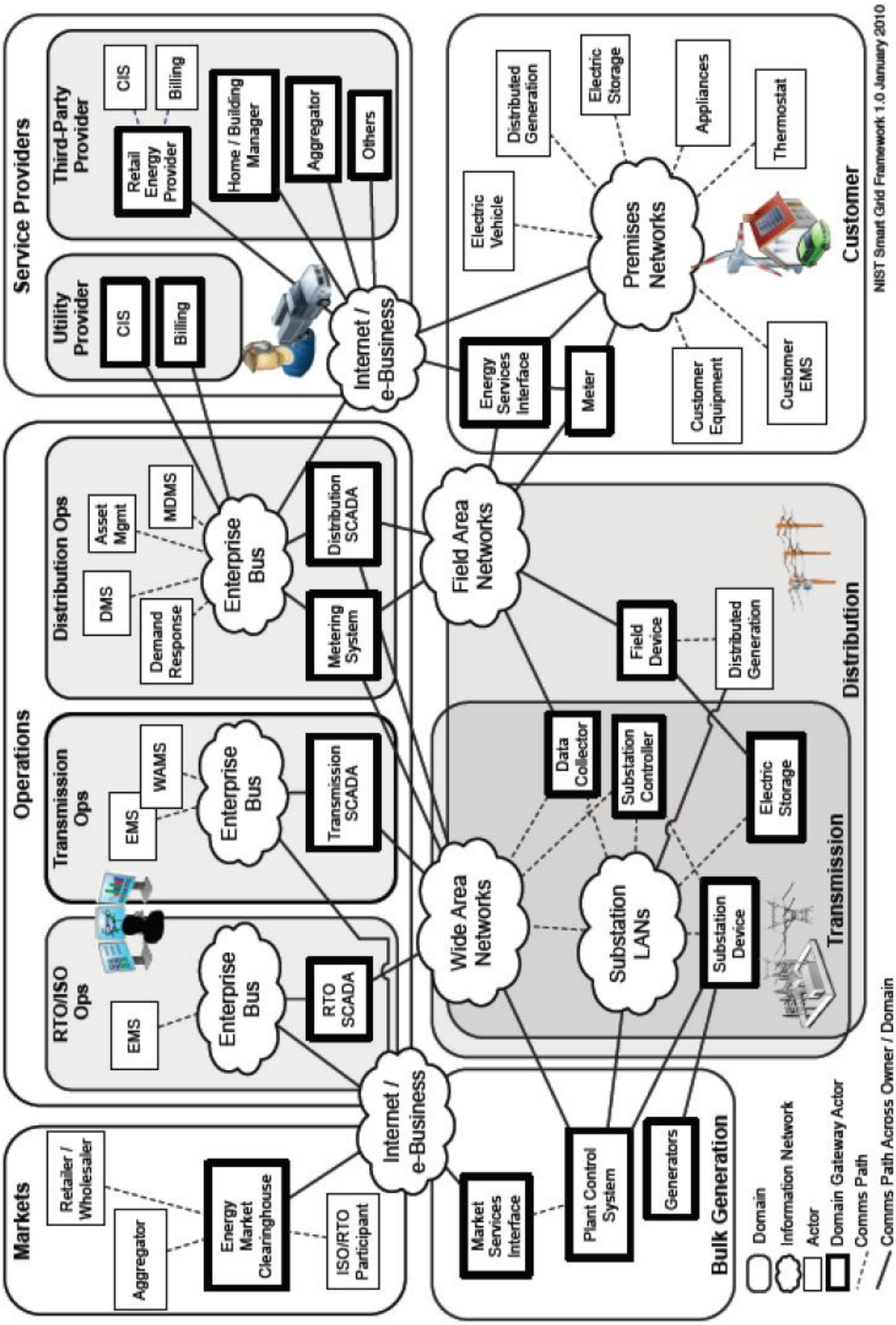

Figure B.3. *The top-level view of conceptual model of Smart Grid [49, p. 35].*

APPENDIX C

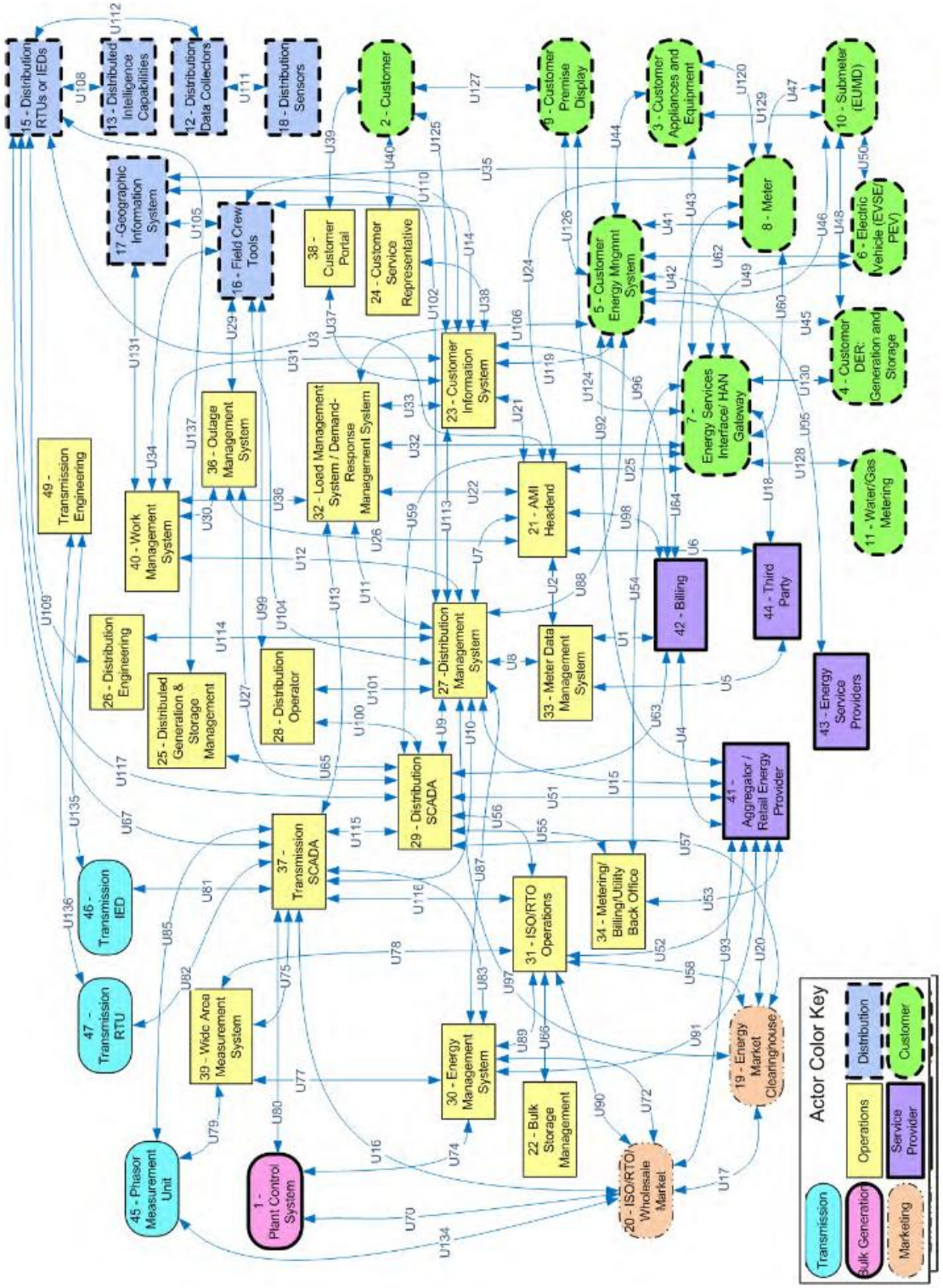

Figure C.1. *Logical reference model [13, p. 17].*

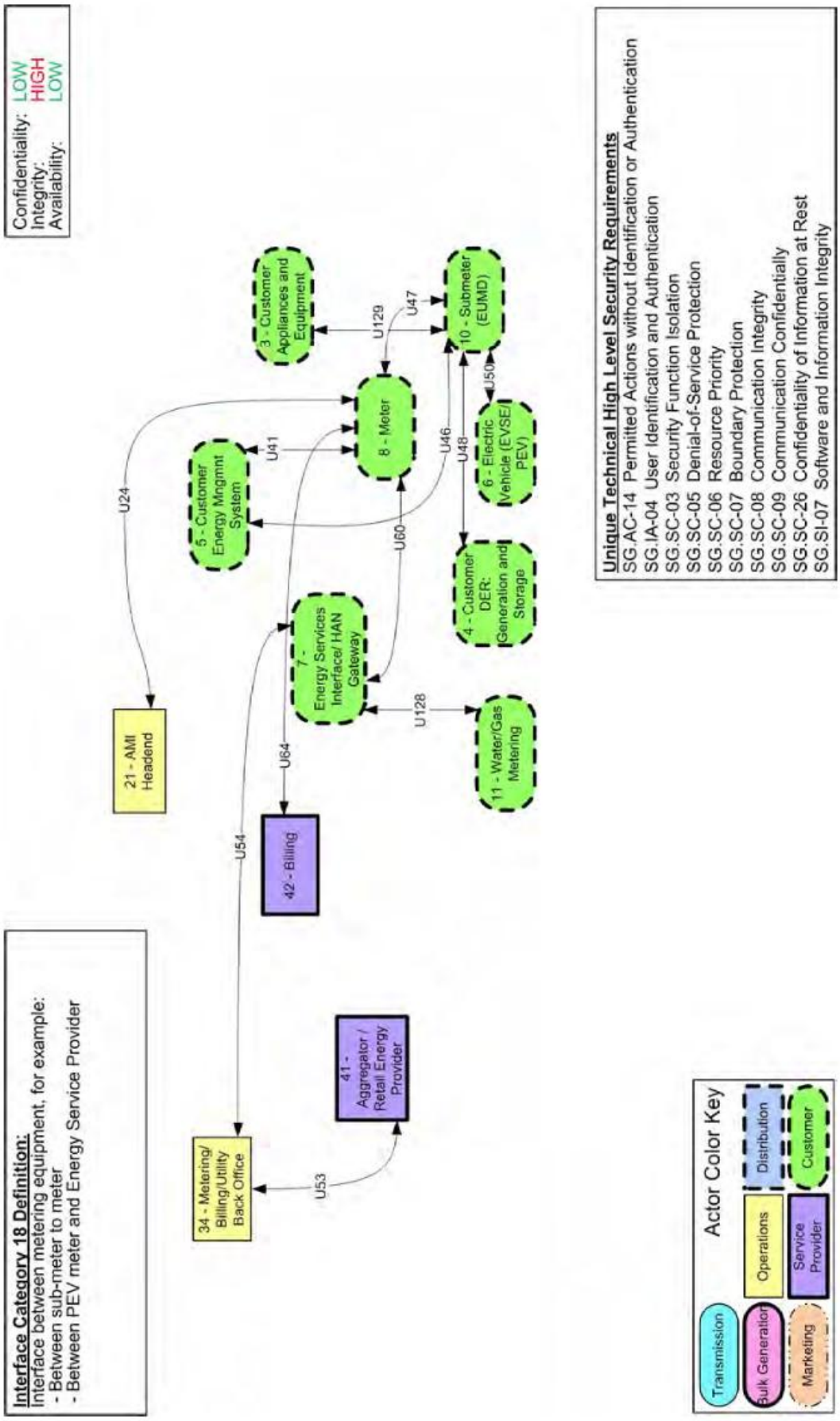

Figure C.2. *Logical interface category 18 [13, p. 64].*

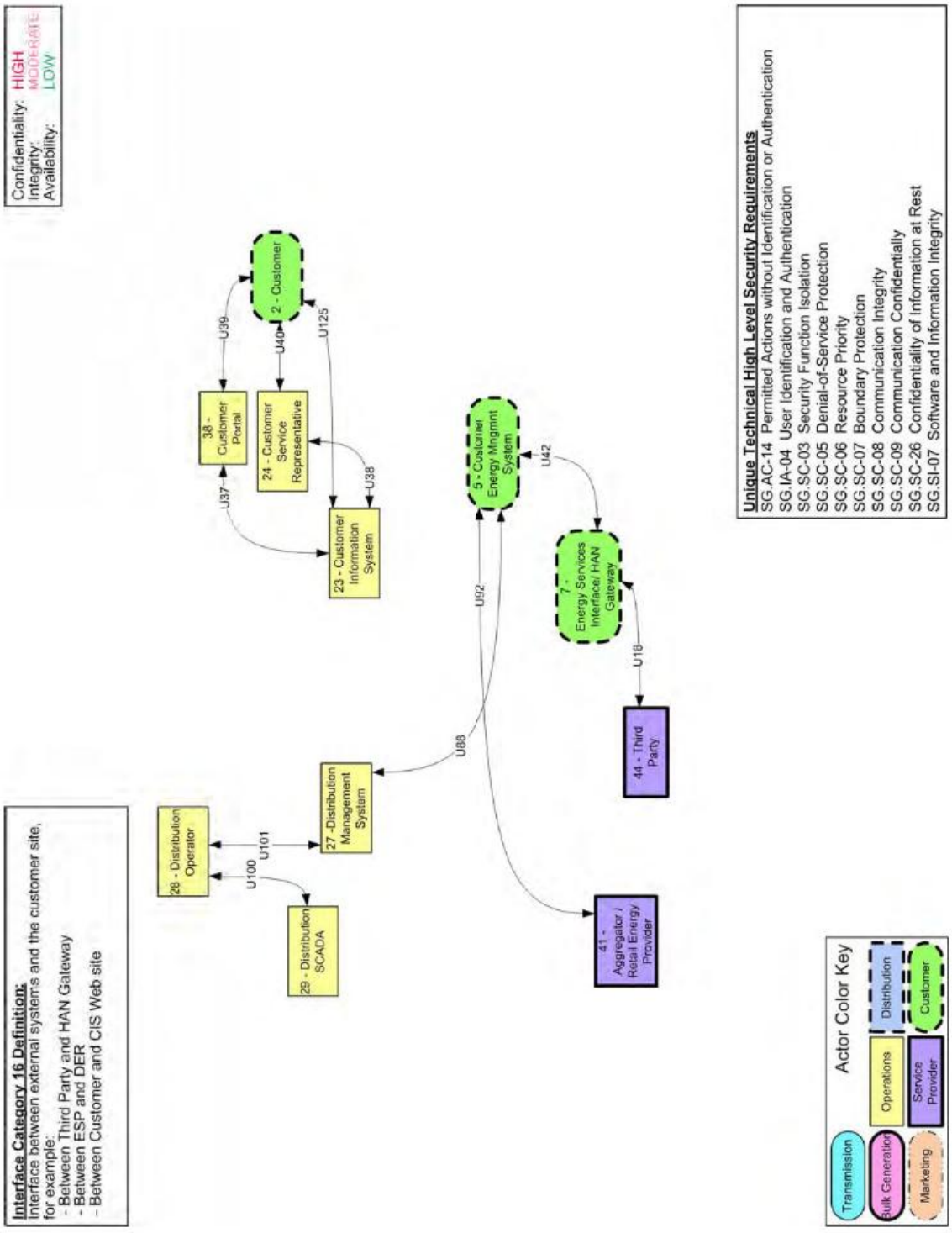

Figure C.3. *Logical interface category 16 [13, p. 59].*

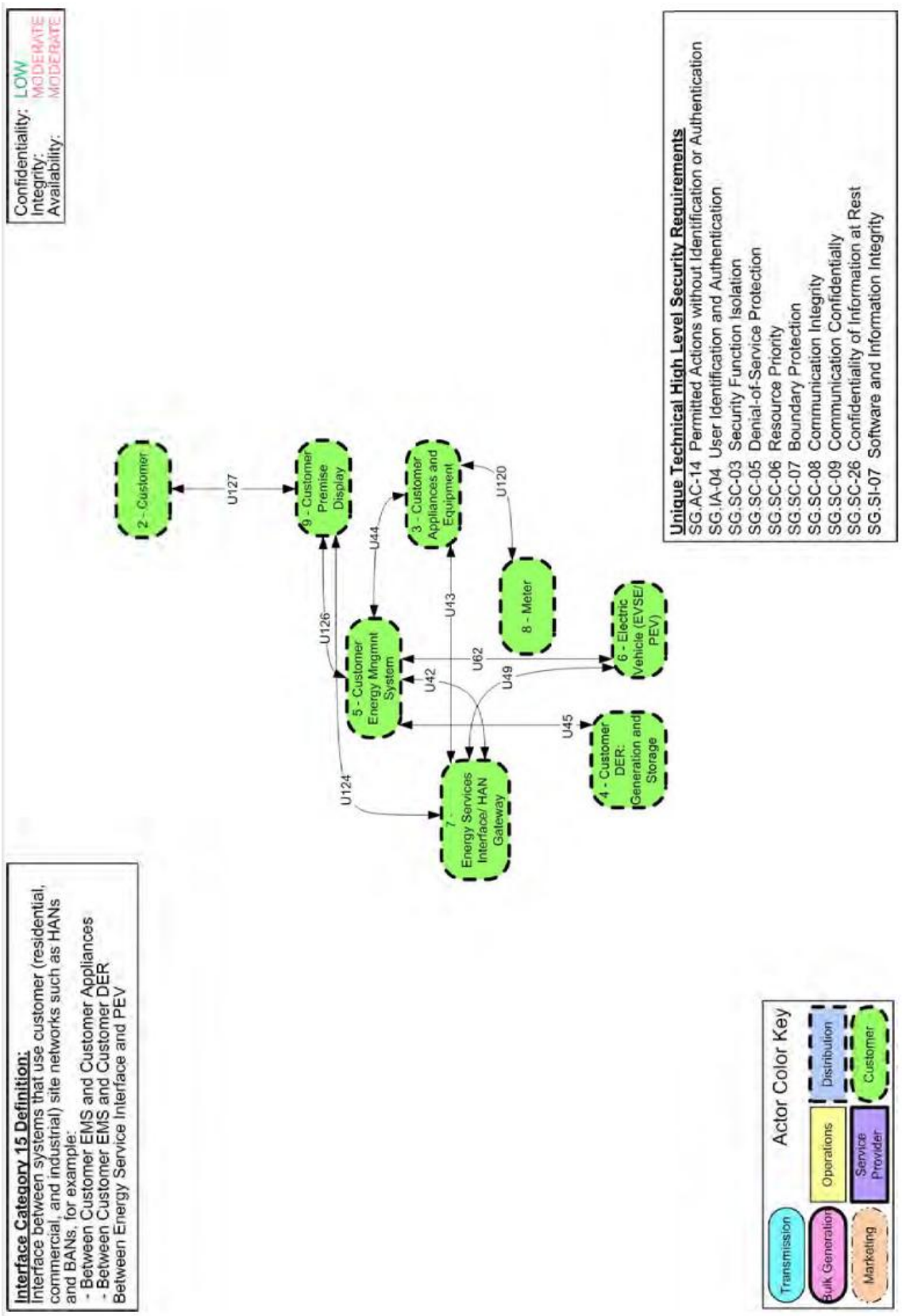

Figure C.4. *Logical interface category 15 [13, p. 56].*