ANALYSING SECURITY ISSUES FOR A SMART GRID DEMONSTRATION ENVIRONMENT

Kim Paananen
TUT[1] - Finland
Finland
kim.k.paananen@gmail.com

Jari Seppälä
TUT - Finland
Finland
jari.seppala@tut.fi

Hannu Koivisto
TUT - Finland
Finland
hannu.koivisto@tut.fi

Sami Repo
TUT-Finland
Finland
sami.repo@tut.fi

ABSTRACT

In this paper we present a way of analyzing and testing information security of smart grid demonstration environment and propose a best practice checklist for information security. 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.

INTRODUCTION

Information security is a crucial part of any smart grid implementation: most of all, it is a part of availability. The paper present the analysis of the demonstration environment through threat modeling and through a closer examination of the demonstration equipment.

The tested system is a laboratory demonstration environment, developed by the Department of Electrical Energy Engineering of TUT in the year 2011 for aggregation of distributed energy resources for network automation and for market based demand response. The demonstration environment includes both the information and the automation systems, as well as the active resources. Fig. 1 presents the overall layout of the demonstration with components and used platforms. More details will be presented later.

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 it is the customer interface. The demonstration environment is of course simpler than the one found in practice.

The threat model of this paper is derived from SANS Threat Modeling principles with smart grid viewpoint. This threat model is made from the end user´s perspective and focuses on the customer domain, especially home energy management system (HEMS).

The testing was done more from a vulnerability assessment point of view than that of penetration testing. The idea of the testing is to simulate a real communication situation, and analyze the information security of that system.

The results from the testing indicate that there are several information security shortages in the demonstration environment. The most serious shortages include unnecessary open ports and services, configuration flaws and vulnerable version of software, information disclosure and protocol flaws, weak encryption and authentication. Vulnerabilities are expected in the system under development. The results from the analysis and testing phase strongly point out the necessity of overall information security analysis during the R&D phase.

The main result of this paper is on showing how this type of analysis should be performed and which things should be taken into account. The proposed top 10 checklist is also a valuable tool when designing security analysis in practice.

APPLIED THREAT MODEL

Smart grids will be complex, integrated systems consisting of sub systems. The two most important sub

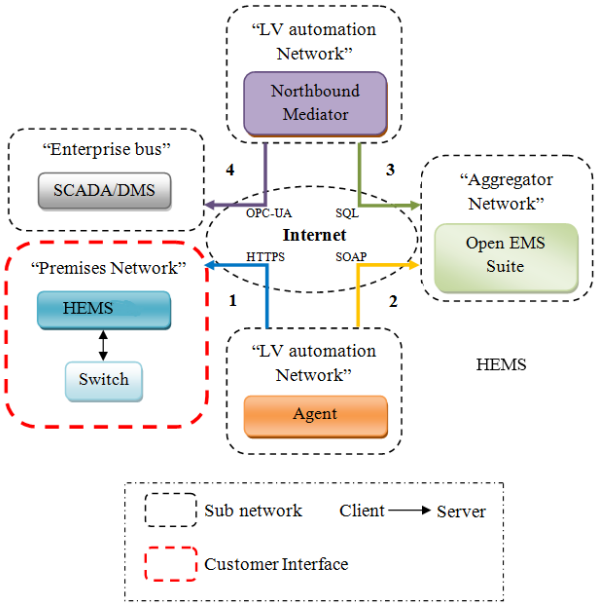

Fig. 1: Simulated testing environment with interfaces.

1) TUT: Tampere University of Technology

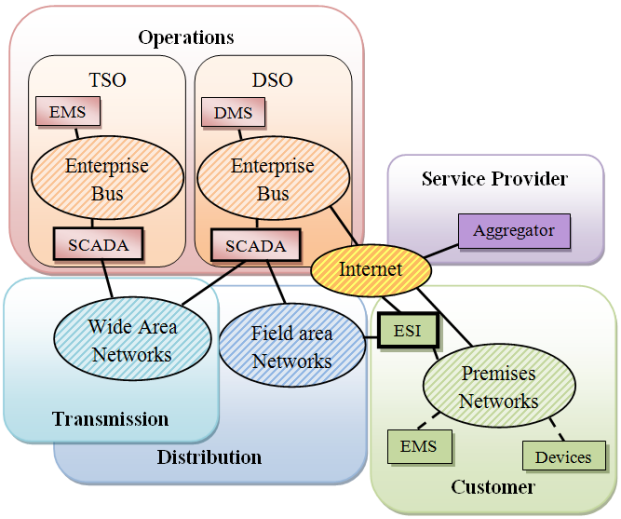

Fig 2: The domains, actors and networks of the simulated environment

systems in regard to information security are the power and ICT systems. 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. However, reaching these objectives will be extremely hard due the complex and altering landscape of information security.[2, p. 4; 8, pp. 35-45.]

The threat model of this paper is derived from SANS Threat modelling principles [4], keeping in mind the smart grid environment. This threat model is made from the end user´s perspective and focuses on the Customer domain, especially HEMS.

Viewing the system as adversary: SGIP/SMWG introduces a logical reference model of smart grid, which contains seven domains and actors with interfaces between them [2, p 17]. See Fig 2.

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.

Successful attacks can change the attitudes against smart grid, especially if people start to think that their security as well as dependability of their home 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.

The third asset, feel of security, is rather connected to other assets. In other words, successful attacks targeted to some assets can lead also to another asset, even though not intended.

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 typical attack vectors consider three situations in which the assets could be reached: the HEMS crashes, work incorrectly, or losses sensitive information.

REVIEW OF THE DEMONSTRATION EQUIPMENT

As a part of Cluster for Energy and Environment (CLEEN) - Smart Grid for Energy Market (SGEM) [9], the Department of Electrical Energy Engineering of Tampere University of Technology (TUT) built a research laboratory demonstration environment of smart grid applications in the year 2011 [3]. This research environment was created to study the aggregation of distributed energy resources for network automation and for network based demand response. It includes both the information and the automation systems, as well as the active resources. Due to the space limitations, only a general overview is presented here.

The ICT system of the laboratory environment consists of distribution network operator control centre software ICS (SCADA/DMS), aggregator (OES), home energy management system (HEMS), and interfaces between these. ICS and OES are already commercial, full-fledged software, whereas the HEMS, Agent, and Northbound Mediators presented in Fig. 1 are still under development.

The main focus of the security review is from the interface of the ICS downwards, all the way to end user's devices. The ICS itself is left to less attention. The most critical information security challenge is the most public multiuser interface. In this case it is the customer interface, and securing the HEMS should, thus, be the number one priority.

HEMS

The used HEMS is basically 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.

Aggregator

The aggregator can be divided into three software components: Agent, OES and Northbound Mediator. OES (Open EMS Suite) 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 HEMS. [3]

The function of Northbound Mediator is to work as an adapter between the OES and ICS systems. In order to communicate with the ICS, Northbound Mediator acts as OPC UA Client, and sends the sum of power demand values to the ICS over an applied OPC-UA TCP protocol.

Industrial control system

The ICS runs on the Control Centre PC (Windows XP), and consists of DMS and SCADA (ABB MicroSCADA Pro DMS 600 and Pro SYS 600). 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 Classic OPC DA and OPC A&E.

Information security analysis

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

DETAILED ANALYSIS AND TEST RESULTS

The testing is done more from a vulnerability assessment point of view than that of penetration testing. This test will concentrate on public interfaces, as they are the most exposed 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 tools used in the testing include Nessus, w3af, Metasploit, Nmap, Tcpdump, Wireshark, Codenomicon Defensics, and Ettercap. These tools have been selected for their suitability and popularity. All, except, Codenomicon´s Defensics, are free of charges to personal usage. Fig. 3 represent how the used tools work on different layers of the OSI model. The actual testing required a lot more time than first calculated and in the end the whole testing was done within six weeks (>100 hours).

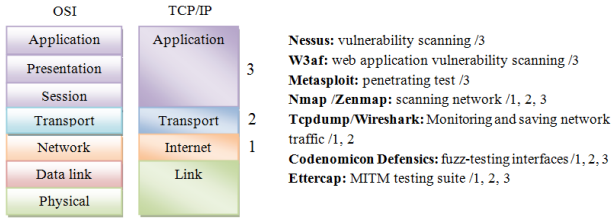

Fig 3: Testing software used in different layers

The results from the testing indicates that there are several information security shortages in the demonstration environment. The most serious shortages include unnecessary open ports and services, configuration flaws and vulnerable version of software, information disclosure and protocol flaws, weak encryption and authentication. 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 1 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. As it can be notices the HEMS is the weakest link in this environment and has many severe flaws, whereas the ICS has been properly configured and do not have that many security holes It should be emphasized that this HEMS system was still under development and observed flaws could easily be fixed for a commercial version.

CONCLUSION

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. Commonly easily fixed items, after analysis.

The most important asset of the system is information, which makes information security the main goal. This

Table 1: Summary of test results divided into groups

Target	Configuration flaw	Software flaw	Implementation flaw
HEMS:	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 authentication. No CA certifications. IP and TCP protocols fail. HTTP protocol failure. Computational constrains, DoS ARP poisoning
OES:	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:	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:	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

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. The challenge is and will be how to enable easy configuration and use of information security features for the end users.

One valuable result is the developed top 10 security checklist. This list has been derived from the test results of the demonstration environment and from various other best practice lists. This checklist is designed for companies and entities that are providing home automation related services or equipment like HEMS in customer domain.

This checklist is available online, together with the main authors (Kim Paananen) M.Sc thesis [5], see http://dspace.cc.tut.fi/dpub/handle/123456789/20985.

REFERENCES

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

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

[3] A. Koto, S. Lu, A. Rautiainen, S. Repo S. & T. Valavaara, 2011, *Demonstration environment for smart grid applications.* Tampere University of Technology - Department of Electrical Energy Engineering. 40p. Available from: http://webhotel2.tut.fi/units/set/research/incapublic/ /tiedostot/Raportit/OES_ThereGate_demo.pdf.

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

[5] K. Paananen, 2011, *Information security in Smart Grid demonstration environment*, M.Sc Thesis, Tampere University of Technology.