Security and Privacy in the SEMIAH Home Energy Management System

T. Gjosaeter, N. Ulltveit-Moe and M. L. Kolhe
University of Agder,
Faculty of Engineering & Science, Norway
Email: {terje.gjosater, nils.ulltveit-moe, mohan.l.kolhe}@uia.no

R. H. Jacobsen and E. S. M. Ebeid
Aarhus University,
Department of Engineering, Denmark
Email: {rhj, esme}@eng.au.dk

I. Introduction

There is an increasing awareness of the importance of energy management in households, and *smart grid* systems are introduced that aim at better utilisation of the energy production and distribution infrastructure. *Home Energy Management Systems* (HEMS) are introduced to shift energy consumption from peak hours to off-peaks where there is high generation of electricity from renewable energy sources. In such a system, *security* and *privacy* is essential.

The SEMIAH project aims to develop a novel ICT infrastructure for implementation of Demand Response (DR) in households. This infrastructure enables the shifting of energy consumption from high energy-consuming loads to off-peak periods with high generation of electricity from Renewable Energy Sources.

The SEMIAH system will include the following elements:

1) A back-end system implementing a virtual power plant which manages and controls information from the households connected to the system network, and which provides intelligent services for energy management of the household;
2) A Home Energy Management Gateway to control customers' loads based on the OGEMA[1] framework;
3) A user interface (smartphone application and consumer web portal) that allows the user to configure the settings of household equipment and add/remove equipment to/from the system.

Elements 2 and 3 represent the front-end system in the user's home. A major concern is securing these two elements and the communication between them, as well as the communication between OGEMA and its managed devices such as heat pumps, stoves and washing machines.

II. Security and Privacy Issues

Several issues may arise with regard to the security and privacy in a smart grid-connected home. When it comes to Denial of service type of attacks, an attacker may block the connection between HEMS and server or attempt to block the user's access to electricity. Other types of attempted sabotage may include to destabilise the grid by turning on or off lots of electrical appliances in the neighbourhood, or even attempting to turn on a user's hot plate from outside, and in worst case create a fire. An attacker may attempt to disrupt the aggregator services or core services in the electricity grid using the HEMS as a bridgehead. Manipulation of electricity meters for reducing the electricity bill, or even attempts to manipulate the electricity market has to be protected against.

Concerning privacy, one should be aware that having legitimate or illegitimate access to the HEMS will enable collection of information about the user such as TV habits and behaviour patterns, and this could be abused for e.g. advertisement purposes. A burglar may also be interested in detecting absence patterns for burglary planning.

III. Architecture Outline

Figure 1 illustrates some possible SEMIAH service scenarios. The primary service scenario is implementing a Demand/Response service for shifting energy usage in time in order to avoid energy usage peaks. This may give some monetary savings for the customer in terms of lower energy price and less high tariff usage where power tariffs are being used. The Demand/Response service will in particular benefit the energy companies, since the Demand/Response system can reduce the need for reinforcing the distribution electricity grid. Demand/response implies measuring energy usage and scheduling energy loads like water boilers, heatpumps, electric vehicles etc. to consume less energy at energy peaks and more energy when there is an excess of renewable energy available.

SEMIAH will also allow for auxiliary services being bundled with the HEMS, for example alarm services or broadband Internet and pay TV services, in order to provide Demand/Response as a value-added service on top of existing services. Another possibility is to have optional value-added services, for example burglar alarm services, running on the HEMS. This means that HEMS applications will need to run in a sandboxed environment, where they only are trusted to access sensors and personal data according to a security and privacy policy. It is also important that auxiliary services and the basic Demand/Response service are well separated, to avoid the risk of attacking the service via weaknesses in these auxiliary services or vice versa.

It is furthermore envisaged that both the Demand/Response and auxiliary services can run in the cloud as Software as a Service (SaaS), using a standardised interface. This will allow

[1] OGEMA – Open Gateway Energy Management Alliance (http://www.ogema.org/)

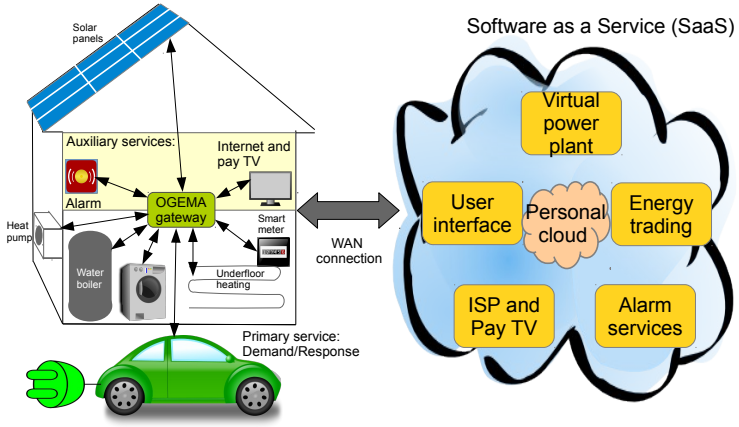

Fig. 1. SEMIAH service scenarios for cloud based operation.

the customer to choose virtual power plant provider based on the best price offer. The virtual power plant and energy trading interface will also run as a cloud-based service, which means that these services must be secured against external attackers and fraud attempts. The security architecture will be based on previous work in the PRECYSE FP7 project, and will be enhanced with multilevel-security based web services which can enforce that sensitive, private or confidential information can be encrypted, so that only authorised stakeholders can access this information. This framework also allows for secure deployment of system configurations and it allows secure web services which only an authorised set of stakeholders can access. This allows for building cloud-based services where critical infrastructure components can be running, and where leakages of sensitive information can be monitored and controlled so that the privacy policies and overall system will improve over time both from a privacy and security perspective.

The user will be able to store private information in Personal Cloud based services, which requires that stakeholders that want to access private data must sign a legally binding link contract in order to use these data. This also means that the customer later can revoke access to private data, if he/she wants to, so that the user is in control of own private data. The architecture will furthermore use existing best security practices for monitoring the cloud-based services (e.g. intrusion detection systems, anti-virus and security testing tools) to ensure that malicious attacks on the HEMS can be detected and in most cases avoided.

IV. Related Work

The PRECYSE[2] project is currently working to define, develop and validate a methodology, an architecture and a set of technologies and tools to improve –by design– the security, reliability and resilience of the ICT systems supporting Critical Infrastructures (CI). SEMIAH will extend and adapt methods and tools from PRECYSE. Because of the constraints on resources in the HEMS and its user interface, we may not be able to use the full PRECYSE toolkit, but will have to select and adapt a suitable subset. In [1], the authors examines security and privacy challenges that arise in smart grids. In [2], the authors present an analysis of security and privacy issues in smart grids operating in cloud-based environments, using the Los Angeles Smart Grid project as a case.

[2]PRECYSE – Protection, prevention and reaction to cyber-attacks to critical infrastructures, funded by the European Commission under the FP7 programme with contract number FP7-SEC-2012-1-285181, http://www.precyse.eu.

V. Discussion and Summary

Best practices and principles such as Security by Design, Privacy by Design, Defence in Depth and Multilevel Security will be taken into account when developing the SEMIAH system, including the HEMS.

As a part of the critical infrastructure, the electricity grid is an essential asset to protect from threats such as cyber-attacks from criminals, terrorists and other potential intruders. Therefore, critical infrastructure cyber-security and current relevant standards will be taken beyond state of the art and adapted to the smart-grid case in order to protect the communication between HEMS, Aggregator and DSO. In addition, the system must offer a high degree of privacy to protect consumer data.

SEMIAH will ensure that requirements, designs and implementations of software, hardware, communication protocols and data handling are in accordance with the intention to create a privacypreserving smart grid solution.

Acknowledgment

The SEMIAH project, *Scalable Energy Management Infrastructure for Aggregation of Households*, is funded by the European Commission under the FP7 programme with contract number FP7-ICT-2013-11-619560, http://www.semiah.eu.

References

[1] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. *Security Privacy, IEEE*, 7(3):75–77, may-june 2009.

[2] Y. Simmhan, A.G. Kumbhare, Baohua Cao, and V. Prasanna. An analysis of security and privacy issues in smart grid software architectures on clouds. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pages 582 –589, july 2011.