SafeBase: A Security Framework for Smart Home Systems Based on Smart Metering Infrastructure

Hannes Raddatz Arne Wall Dirk Timmermann

Institute of Applied Microelectronics and Computer Engineering, University of Rostock
18051 Rostock, Germany, Tel.: +49 381 498-7271
{hannes.raddatz, arne.wall, dirk.timmermann}@uni-rostock.de

Abstract

Current Smart Home systems are often based on proprietary security solutions which hide its inner functionality and possible vulnerabilities until they are exploited. Furthermore, an initial trusted instance in Smart Home networks is necessary to provide a seamless trust relationship to Smart Home appliances. Another issue is the stalling roll-out of Smart Metering systems due to its bad price-performance ratio for the customer. Therefore, we provide the lightweight security framework SafeBase, which solves both issues and provides a possible solution for a future Smart Home and Smart Metering systems. To achieve this goal, we employ state-of-the-art protocols like Constrained Application Protocol (CoAP), Object Security for Constrained RESTful Environments (OSCORE), Authentication and Authorization for Constrained Environments (ACE) and LwM2M.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General

General Terms

IoT Security, Authentication, Authorization

Keywords

Smart Home, COAP, OSCORE, ACE, Smart Metering

1 Introduction

Current Smart Home systems are often based on proprietary security solutions which hide its inner functionality, often called ”security through obscurity”. Consumers have to trust the device manufacturer that their Smart Home system is secure. It is impossible to check whether the system meets Kerckhoffs' Principle (even if the attacker knows the algorithm of the security mechanism, he is not able to break into the system). Consequently, existing vulnerabilities are rarely discovered before they are exploited. Following this, an open-source implementation can overcome this disadvantage and allows the development of a future-proof system. Another key development leading to the proposed concept, is the worldwide roll-out of Smart Metering systems. Currently, installing such a Smart Metering system doesn't provide a benefit for the tenant, except that the meter readings do not need to be reported periodically. However, the tenant/owner has to pay for the acquisition and installation of such a Smart Metering system. Opening the Smart Metering system to customers by utilizing its cryptographic features for the Smart Home network can fundamentally change the acceptance rate of Smart Metering systems and introduce a new way of securing Smart Home systems in the future. By using state-of-the-art protocols for the Internet of Things (IoT) like CoAP, OSCORE, ACE and LwM2M (details in section 2.2) a reference security framework for Smart Home systems can be realized.

International Conference on Embedded Wireless
Systems and Networks (EWSN) 2018
14–16 February, Madrid, Spain

ISBN: 978-0-9949886-2-1

2 Concept

This section describes the design of the security framework SafeBase. First, the network and metering infrastructure of a generic apartment building is presented in section 2.1. It follows in section 2.2 an introduction to the software structure and protocols used by the proposed framework.

2.1 Network and Metering Infrastructure

Typical Smart Metering systems consists of Smart Meters for each apartment and energy source, e.g., electricity and gas as well as a Smart Meter Gateway. The latter one acts as a broker between the local meters and energy providers. For this purpose, it handles the communication over an wide area network (WAN) and provides security and cryptographic features. The WAN access is provided, among others, via a cellular interface or power line communication (PLC). In Germany, each Smart

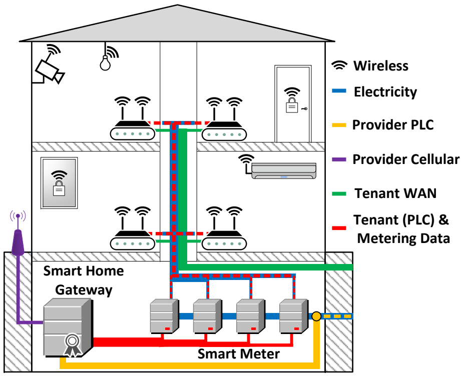

Figure 1. Apartment building with Smart Homes appliances and upgraded Smart Metering infrastructure.

Meter Gateway has to be certified by an accredited test center of the Feral Office for Information Security (BSI) according to a specific Protection Profile and related technical guidelines [1]. Key requirement is a security module with cryptographic algorithms in hardware, a strong random number generator and a secure storage for secrets and certificates. Currently, Protection Profile and guidelines allows tenants only read access for metering values. Our proposed upgrade of a Smart Meter Gateway to a Smart Home Gateway (SHGW) utilizes the in-build security module for value-added services of the tenants Smart Home system. To achieve such a functionality, a communication between the tenants network, respectively a router, and the SHGW needs to be established. Currently, there is no official guidance to assess such a connection. In our concept, we propose a power line communication to reduce installation costs. In future, this can be achieved by PLC-capable routers and Smart Meters for electricity, as shown in figure 1.

2.2 Framework

The proposed concept shall serve as a lightweight security framework for developers of Smart Home applications.

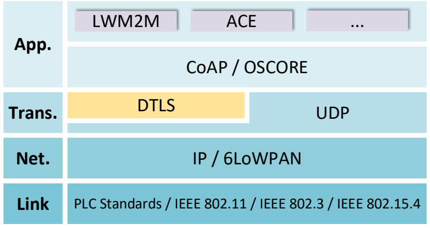

Figure 2. SafeBase protocol stack

In this section, we explain the selection of the protocols. Figure 2 shows the protocols used in the framework arranged by layers of the TCP/IP stack. At the link layer, power line communication is used in our example in figure 1 for communication between apartment routers and SHGW (IEEE 1901, HomePlug). As well as between SHGW and energy provider (IEEE 1901, various ITU standards). While IEEE 802.3 Ethernet is used in some scenarios, major protocols for Smart Home are IEEE 802.11 WLAN [2] (user devices) and IEEE 802.15.4 [3]. If both wireless protocols are used in the same network, a gateway is necessary to interconnect devices beyond protocol borders. At the network layer,the Internet Protocol (IPv4/v6) or the superset profiles 6LoWPAN [3] and ZigBee can be used. The profiles are designed for embedded devices using IEEE 802.15.4 on link layer. On top of that, the User Datagram Protocol (UDP) realizes a lightweight and connection-less transport layer, which leaves the retransmission meachanism to the application layer protocol. Depending on the upper layer protocol, Datagram Transport Layer Security (DTLS) [6] will be used to warrant integrity, confidentiality and authenticity of the communication. The framework utilizes on application layer the Constrained Application Protocol (CoAP) [5], which is a popular RESTful protocol and in competition with MQTT, a broker based protocol, as the top choice for sensor networks. The CoAP standard recommends DTLS to secure the communication. However, it also lists the drawbacks of using CoAP combined with DTLS, e.g., no support for group communication and potential security vulnerabilities when using proxies (no end-to-end encryption) [5]. To overcome these limitations, the draft Object Security for Constrained RESTful Environments (OSCORE) was originated. It introduces the flexible object-security concept (clear text, partly or complete encrypted mode can be select for each message type) to CoAP by utilizing CBOR Object Signing and Encryption (COSE) [5] and solves the mentioned problems. Therefore, it is an interesting candidate for a Smart Home security framework. On top of this protocol stack, we will use Authentication and Authorization for Constrained Environments (ACE) [4], an IoT framework to manage access control permissions in Smart Home and IoT scenarios. ACE is based on OAuth2.0 and defines the roles authorization server (AS), resource server (RS) and client. The SHGW will act in our concept as the main AS, while Smart Home appliances and user devices, e.g., a smartphone, represent RS or client depending on the scenario. A user device will be assigned to a specific tenant during a one-time procedure in front of the SHGW. A successful completion of this procedure allows the user to add new devices to the Smart Home system of his apartment by using the assigned user device. Such activities will be logged to track potential misuse. Based on ACE, a comprehensive access and automation rule management will be realized. Additionally, this allows to revoke already granted permissions, if necessary. The SHGW with its certified security features will act in such a scenario as a certificate authority (CA) and maintain a public key infrastructure for Smart Home appliances. Furthermore, maintenance is an important topic to enable long-term security. For this purpose, a device management protocol called LwM2M from the Open Mobile Alliance will be integrated into our framework. It uses CoAP to enable remote management of devices. This allows, among others, an automation of firmware upgrades for devices in the Smart Home to patch vulnerabilities.

3 Conclusion

Currently, we develop prototype implementations and specific demonstration devices. For example, a remote audio and video doorbell and a user device authorization process in conjunction with an identity check of the tenant by utilizing the new electronic German national Identity Card. Furthermore, the performance of mesh structures according to IEEE 802.11s [2] and conceptual approaches emerging from it will be investigated.

4 Acknowledgments

We would like to thank the German Federal Institute for Research on Building, Urban Affairs and Spatial Development (BBSR) for their support in this project. This work is partially granted by BBSR within the scope of project ”Zukunft Bau”.

5 References

[1] BSI PP and BSI SMGW PP. Protection profile for the gateway of a smart metering system. Technical Report March, 2011.

[2] G. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke. IEEE 802.11s: The WLAN Mesh Standard. *IEEE Wireless Communications*, 17(1):104–111, feb 2010.

[3] G. Montenegro, J. Hui, D. Culler, and N. Kushalnagar. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, Sept. 2007.

[4] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig. Authentication and Authorization for Constrained Environments (ACE). Internet-Draft draft-ietf-ace-oauth-authz-08, IETF, Oct. 2017.

[5] G. Selander, J. Mattsson, F. Palombini, and L. Seitz. Object Security for Constrained RESTful Environments (OSCORE). Internet-Draft draft-ietf-core-object-security-06, IETF, Oct. 2017.

[6] Z. Shelby, K. Hartke, and C. Bormann. The Constrained Application Protocol (CoAP). RFC 7252, June 2014.