Criteria for Security Classification of Smart Home Energy Management Systems

Manish Shrestha[1,2], Christian Johansen[1], and Josef Noll[1]

[1] University of Oslo, Oslo, Norway, cristi@ifi.uio.no, josef@jnoll.net
[2] eSmart Systems AS, Halden, Norway, manishsh@student.matnat.uio.no

Abstract. Internet of Things (IoT) is a growing field and its use in home automation is no exception. However, the end users lack security awareness whereas the system designers lack the incentives for building secure IoT systems. To address this challenge, we propose the notion of security classes to assess and present the security of complex IoT systems both for the users and for developers. Furthermore, regulatory bodies can use our security classification method as a reference to derive requirements for adequate security. This paper extends the previous security classification methodology towards Smart Home Energy Management Systems (SHEMS). We demonstrate its applicability by performing a systematic security classification assessment of an industrial SHEMS. Results show that the use of security classes can give a good indication of security status and guidance to improve the security of IoT system.

Keywords: Security Classification, Exposure, Security assessment, Cybersecurity, Smart home, IoT

1 Introduction

The proliferation of IoT has created new transformative opportunities s.a. observed with smart homes [1, 14]. Today, the applications inside smart homes are more than luxury, where, e.g., energy management systems can enable efficient utilization of energy [4]. Industrial IoT providers are normally concerned with the development of functionalities, creating a range of communication and sensing capabilities integrated into small devices. However, security and privacy have been a major concern, which often hinders a wider adoption of IoT systems.

This paper is an extension of our previous work [12] where we introduced a general security classification methodology for smart grid systems. In this paper, we extend the security classes with details regarding connectivity classes and protection mechanisms suitable for Smart Home Energy Management Systems (SHEMS) and show the application of our approach to an existing commercial system. One motivation of the present work is to help companies to improve and maintain IoT security of their products guided by security classes and the protection mechanisms that they specify.

We describe in Section 2, the reference architecture for SHEMS that we follow, and briefly introduce the system from our case study. Our main contribution is presented in Section 3 where we extend the security classification method towards SHEMS. We show the application of this new methodology in Section 4 using a case study of existing SHEMS from Develco Products.

2 A Commercial Home Energy Management System

A SHEMS is a smart home system dedicated to saving energy by monitoring and managing electrical appliances, which may include load, storage, or generation resources [6,7,15]. Functional modules of SHEMS may include monitoring, logging, control, management, or alarm services [15]. Ghirardello et al. [5] summarize a smart home reference architecture (see Fig. 1) by integrating three different viewpoints: functional, physical, and communication. Based on this architecture, we describe the major components of smart home systems as below.

IoT Devices. These have as primary functions [5] to sense the environment, transfer data, and receive commands. As such, these have communication capabilities and may be able to interact with other components of the Home Area Network (HAN) such as IoT hubs, residential gateways, or other IoT devices. In SHEMS, IoT devices may include metering (and sensing) devices and controllable loads.

IoT Hub. It acts as a central controller of IoT devices as well as a bridge between these and the backend system. Sensor data is reported to the IoT hub, which translates and sends it to the backend system. Similarly, the IoT hub may receive control commands, which it can relay to the intended devices. Opposed to IoT devices, the IoT hub has considerably more computing capability and can make decisions to manage and control the IoT devices.

Residential Gateway. It is a bridge to connect IoT devices to the Internet [5], i.e., between the HAN and the Wide Area Networks (WAN). In some systems, a gateway may act as an IoT hub or vice versa.

Communication Channels. A SHEMS consists of two types of networks: HAN and WAN. The HAN is formed of the sensors and the IoT hub, and utilize wireless communication links s.a. Zigbee, Z-Wave, Wireless M-Bus, Thread [3,5]. The IoT hub and devices may also utilize Wi-Fi or Ethernet to connect with the residential gateway. In a WAN, a SHEMS typically utilizes home internet provided by internet subscribers or cellular networks to communicate with the backend system.

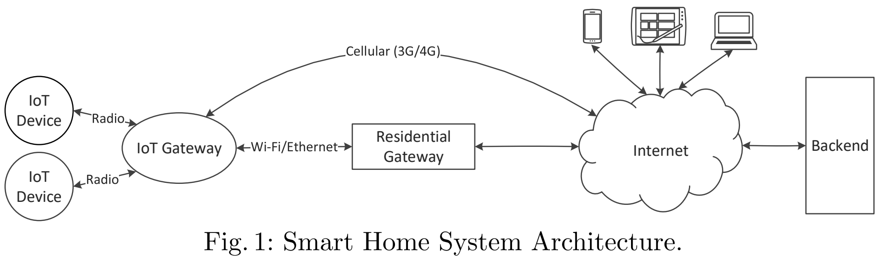

Fig. 1: Smart Home System Architecture.

Backend System. It is a centralized component, which manages several smart homes, and resides remotely, communicating with the IoT hub through the Internet and performing storage, monitoring, and control functionalities of IoT devices. Backend systems provide an interface to external applications through APIs, enabling communications with SHEMS [14].

Application and Network Data. The network data includes mainly information related to connectivity, whereas application data are those which actually have business value and include meter values, commands for controlling devices, log data, firmware image files, etc. Metered values are produced by IoT devices and sent to the IoT hub, which further sends these to the backend systems for storage and analysis. On the other hand, control commands are received by the IoT hub from the backend system and then sent to the IoT devices for execution.

We apply our security classification to the commercial smart home solution offered by E2U Systems AS, who use hardware provided by Develco Products and implement customized software solutions for smart homes. The Develco Products offer an IoT hub (called *Squid.link gateway*) and a variety of IoT devices such as smart plugs, sensors, alarms, meter interfaces, etc. The IoT hub is able to act as a residential gateway using the cellular network, and it also provides an Ethernet and a WLAN interface for Internet connection as well as a USB interface for plugging in 3G/4G dongles. The Squid.link gateway is a modular platform capable of bridging multiple wireless platforms, like Zigbee, Z-wave, Wireless M-Bus, in the HAN network. The wireless module on the main board of the IoT gateway communicates with the CPU using the SmartAMM protocol, which is the proprietary protocol that also facilitates communication between gateways and the backend system.

3 Extended Security Classification Method

The Smart Grid Security Classification (SGSC) methodology [12] is based on the ANSSI classification method [2]. However, instead of estimating the exposure based on the complexity of the system and attacker model (as in ANSSI), the SGSC combines the *connectivity* (which captures the surface of a system exposed to attacks) with *protection* (which describes the mechanisms of the system used to protect various part of the connectivity surface). Figure 2 summarises how a security class would then be computed. The computation first looks at the components of the system and then aggregates the results upwards until reaching the full system. Notably, the SGSC does not focus on attackers, as classical risk-based methods do, but is concerned instead with how a system can be securely built from the design phase. The benefit is that the SGSC helps system designers to choose the best security functionalities to meet their goal security class.

We consider two types of exposures: IT Exposure and Physical Exposure. For both, we evaluate the connectivity into one of five levels as follows:

C1 : Includes completely closed/isolated systems.

C2 : Includes the system with wired Local Area Network and does not permit any operations from outside the network.

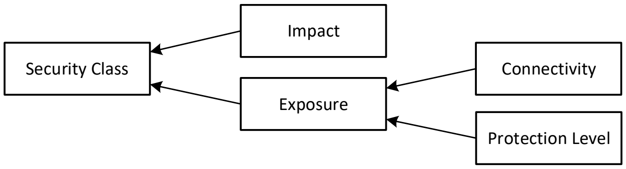

Fig. 2: Methodology of computing a security class [12] (Impact is as in ANSSI).

Table 1: Calculations of (a) Exposure Levels and (b) Security Classes

P1	E4	E4	E5	E5	E5
P2	E3	E4	E4	E5	E5
P3	E2	E3	E3	E4	E4
P4	E1	E1	E2	E2	E3
P5	E1	E1	E1	E1	E2
Protection/ Connectivity	C1	C2	C3	C4	C5

Catastrophic	A	C	E	F	F
Major	A	B	D	E	F
Moderate	A	B	C	E	E
Minor	A	A	B	D	D
Insignificant	A	A	A	C	C
Impact/ Exposure	E1	E2	E3	E4	E5

C3 : Includes all C2 systems that also use wireless technologies.
C4 : Includes the system with private or leased infrastructure, which may permit remote operations (e.g., VPN, APN, etc).
C5 : Includes distributed systems with public infrastructure, i.e., like the C4 category except that the communication infrastructure is public.

We have defined Protection Levels (P) to capture the strength of security functionality implemented in a system. Protection Levels have been inspired by the Safety Integrity Levels (SIL) [10]. Instead of the attacker model, we consider the connectivity of the system when setting the required security mechanisms. Each security mechanism possesses a different strength level which can be ranked. We have defined five protection levels, where P1 represents no protection and P5 represents the strongest protection mechanisms. Table 1(a) shows the evaluation of exposure level from connectivity and protection level. The evaluation of the protection level is conducted by security experts.

In [12] we have not considered protection mechanisms in detail (the same as how standards like ANSSI also do). In this paper, we detail this important part

Table 2: Referred sources for the construction of security criteria.

Protection Criteria	**Source**
Data Encryption	ISO 27002, OWASP, ETSI
Communication and Connectivity Protection	IIC, ISO 27002, ETSI
Software/Firmware Security	ISO 27002, OWASP, ETSI
Hardware-based Security Controls	CSA
Access Control	ISO 27002, OWASP, IIC, CSA, ETSI
Cryptography Techniques	IIC, ISO 27002
Physical and Environmental Security	ISO 27002, OWASP, CSA
Monitoring and Analysis	ISO 27002, OWASP, IIC, CSA, ETSI

of our SGSC by ranking various security functionalities, focusing on our SHEMS application domain. Table 2 lists classes of functionalities.

We extend [12] by extracting the security criteria for evaluating protection levels based on the following standards and best practices:

ISO 27002 which however does not cover the IoT systems;
CSA the IoT Working Group of the Cloud Security Alliance;
IIC the Industrial Internet of Things Volume G4 Security Framework;
OWASP "IoT Security Guidance"; and
ETSI TS 103 645 "Cyber Security for Consumer Internet of Things".

We detail further the security criteria with security functionalities inspired by the IoT Security Compliance Framework proposed by IoT Security Foundation (IoTSF), which is in the form of a checklist. Table 3 shows the mapping of security criteria to security functionalities and protection level.

4 Applying the Security Classification to SHEMS

The SHEMS in our case complies with the reference architecture from Section 2 and consists of a centralized IoT hub and smart plugs connected to controllable loads s.a. water heater, air conditioner, floor heating, etc. For simplicity, we do not include the storage batteries that can act as both load and generation device. We first identify the criticality (**Impacts**) of successful cyberattacks on SHEMS.

Safety. Leakage of data from SHEMS may disclose the presence of people inside their house, which may result in burglary or worst. Moreover, residents may feel unsafe (reducing trust in SHEMS) if they realize they are being watched.

Grid imbalance. During the execution of a demand response program, devices that utilize higher energy are turned off to shave the peaks. If an attacker can switch on/off a large number of loads, these may use unexpected amounts of energy that may destabilize the grid [8, 13].

Increased electricity bills. Compromising SHEMS may result in equipment being switched on without authorized persons noticing.

Privacy. Data from SHEMS can be privacy sensitive, e.g., [9] have demonstrated that mere high-frequency consumption data can be exploited to derive private information s.a. number of people in the house, sleep routines, the presence of babies at home, etc. Compromised SHEMS data may contain even more detailed information. Stealing such data may result in the exposure of personal habits of the residents, which may impact social reputation.

Agents for other cyberattacks. Typically, smart home gateways have connectivity to the Internet. A compromised gateway may act as a bot to launch several other attacks.

Among the aforementioned impacts, grid imbalance and agents for other cyberattacks can be considered as major impacts as these may result in blackouts and damage of physical infrastructures. The remaining impacts could be considered moderate or minor.

We limit the presentation of the application of security classification only to Application and Network Data, in particular, we assess the Command and

Table 3: Protection Level Requirements

Protection Criteria	Security Functionality	P5	P4	P3	P2
Data Encryption	Encryption of data between system components	x	x	x	x
	Strong encryption mechanism	x	x	x	
	Credentials should not be exposed in the network	x	x	x	
	End-to-end encryption	x	x		
	Should not use custom encryption algorithms	x	x		
	Sensitive stored data should be encrypted	x	x		
Communication and Connectivity Protection	Have a minimal number of network ports open	x	x	x	
	Devices should not be accessible from the Internet	x	x	x	
	Only authorized components can join the network	x	x	x	
	Use only standard communication protocol	x	x		
Software /Firmware Security	Updatability of device firmware	x	x		
	Updatability of the operating system	x	x		
	Automatic updates available	x	x		
	Encryption of update files	x	x		
	Signing update files before installing	x	x		
Hardware-based Security Controls	Using Trusted Platform Modules (TPM)	x	x		
	Use of Memory Protection Units (MPUs)	x	x		
	Incorporate Physically Unclonable Functions	x	x		
	Use of Cryptographic Modules	x	x		
Access Control	Disable remote access functionality	x			
	Only authorized devices can join the network	x	x	x	
	Default and weak passwords should not be used	x	x	x	
Cryptography Techniques	Secure bootstrapping	x	x		
	Secure key generation	x	x		
	Secure key storage	x	x		
	Secure key distribution	x	x	x	
	Secure key rotation	x	x		
	Message integrity	x	x	x	
Physical and Environmental Protection	Tamper resistance	x	x		
	Minimal physical ports available	x	x	x	
	Physical security of connections	x	x	x	
	Ability to disable external ports and only minimal ports enabled	x	x		
	Only authorized physical access	x	x	x	
Monitoring and Analysis	Monitoring system components	x	x		
	Analysis of monitored data	x	x		
	Act on analysed data	x			

Control (C&C) for a demand response program, which is one of the most critical components of SHEMS. We apply the classification method in two scenarios.

Scenario I: Centralized Control. In this scenario, Distribution System Operators (DSO) have an agreement with consumers to control the SHEMS appliances to properly manage peaks of energy demand. In our system, each controllable device is plugged into the corresponding smart plug and depending on the device and their maximum effect, rules for controlling them are defined, e.g., a water heater with a maximum capacity 3kW can be controlled only between 8:00 AM to 6:00 PM during weekdays, and once turned off, it cannot be turned on for minimum 15 minutes. The DSOs forecast the energy demand in advance and if reductions are needed at given times, DSOs optimally select the devices to be turned off for a given duration to meet the goal of targeted reduction of consumption and control commands are sent to the selected devices.

Class Evaluation. The connectivity between the IoT device and the hub is C3 (cf. Section 3) and between the hub and the backend system is C5. If an attacker is able to manipulate the device control only inside the HAN (C3), the impact is only Minor. However, if an attacker is able to trigger or manipulate the message for the demand control program from the backend (C5), several devices can be turned off, resulting in grid imbalance as discussed above. As a result, for this scenario, we evaluate the overall impact as Major.

To evaluate the security class, we first select the relevant security criteria for C&C as Data Encryption, Communication and Connectivity Protection, Access Control, and Monitoring and Analysis. We then evaluate the protection level based on the strength of the security functionalities in the selected criteria. Due to space limitations, we do not discuss here our specific evaluations, but provide details in the technical report [11]. Using Table 3 we assign the overall protection level P4.

Using Table 1(a) we determine from the computed values of connectivity (C5) and protection level (P4), the exposure E3. Using Table 1(b) we get the class D (Impact Major and Exposure E3), which is a poor score not suitable for SHEMS. To improve the security class, Table 1(b) indicates that either exposure or impacts need to be reduced. Similarly, exposure can be reduced either by increasing the protection level or by reducing the connectivity, cf. Table 1(a).

Scenario II: Edge Control. In this scenario, the control signals are sent by the IoT hub autonomously, based on the time of peak demand or price of electricity, and thresholds set by the end-user. Users can also set priorities for the devices that need to be controlled and rules to decide e.g., when and how long the devices can be controlled. Thresholds and rules can also be persisted in the IoT gateway so to control the devices without requiring interaction with the backend.

Class Evaluation. Similarly, if an attacker can manipulate the control message within the HAN network (C3), the impact is considered as Minor. However, since there is no flow of commands from the backend system, an attacker cannot influence many devices on a large scale. Since there are no changes in the protection mechanisms, we can consider it as P4. Moreover, using Table 1(a), we obtain the Exposure E2 and using Table 1(b) we computed the security class as A.

The analyses of scenario I and II showed that by moving from the centralized control to the edge control for the demand control functionality, the security class of the demand control is significantly improved from class D to class A. In addition, scenario II may even be more efficient and have lower latency because the trigger of device control initiates locally rather than from the backend system to several IoT devices. Such improvements in the design of IoT systems should be considered to improve the security of the overall system.

5 Conclusion and Further Work

We present the security classification methodology extended with details regarding security functionalities relevant for SHEMS. We have applied this methodology to the commercial SHEMS from our collaborators E2U, and presented in this paper how we performed the assessment of the component for control and command of the SHEMS within demand and response programs. We have first evaluated the security class of the C&C for a centralized control architecture and then saw that the classification methodology can give indications of the possible changes in the design of the system to improve the security class (as in our second scenario). Further work can focus on aggregation mechanisms for calculating the overall system security class from its components.

References

1. Aldrich, F.K.: Smart homes: past, present and future. In: Inside the smart home, pp. 17–39. Springer (2003)
2. ANSSI: Classification Method and Key Measures (2014)
3. Celebucki, D., Lin, M.A., Graham, S.: A security evaluation of popular internet of things protocols for manufacturers. In: ICCE, pp. 1–6. IEEE (2018)
4. Fitriaty, P., Shen, Z., Sugihara, K.: How green is your smart house: Looking back to the original concept of the smart house. In: Green City Planning and Practices in Asian Cities, pp. 39–76. Springer (2018)
5. Ghirardello, K., Maple, C., Ng, D., Kearney, P.: Cyber security of smart homes: Development of a reference architecture for attack surface analysis (2018)
6. Lee, J.I., Choi, C.S., Park, W.K., Han, J.S., Lee, I.W.: A study on the use cases of the smart grid home energy management. In: ICTC, pp. 746–750. IEEE (2011)
7. Liu, Y., Qiu, B., Fan, X., Zhu, H., Han, B.: Review of smart home energy management systems. Energy Procedia **104**, 504–508 (2016)
8. Mohsenian-Rad, A.H., Leon-Garcia, A.: Distributed internet-based load altering attacks against smart power grids. IEEE Trans. Smart Grid **2**(4), 667–674 (2011)
9. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private memoirs of a smart meter. In: Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building, pp. 61–66. ACM (2010)
10. Redmill, F.: Understanding the use, misuse and abuse of safety integrity levels. In: 8^{th} Safety-critical Systems Symposium, pp. 8–10 (2000)
11. Shrestha, M., Johansen, C.: Criteria for Security Classification of Smart Home Energy Management Systems (long version). Tech. Rep. 476, Uni. Oslo (2019)
12. Shrestha, M., Johansen, C., Noll, J., Roverso, D.: A Methodology for Security Classification applied to Smart Grid Infrastructures. International Journal of Critical Infrastructure Protection (IJCIP) (2019). (to appear)
13. Soltan, S., Mittal, P., Poor, H.V.: Blackiot: Iot botnet of high wattage devices can disrupt the power grid. In: 27th USENIX Security Symposium, pp. 15–32 (2018)
14. Stojkoska, B.L.R., Trivodaliev, K.V.: A review of internet of things for smart home: Challenges and solutions. Journal of Cleaner Production **140**, 1454–1464 (2017)
15. Zhou, B., Li, W., Chan, K.W., Cao, Y., Kuang, Y., Liu, X., Wang, X.: Smart home energy management systems: Concept, configurations, and scheduling strategies. Renewable and Sustainable Energy Reviews **61**, 30–40 (2016)