UiO : Department of Informatics
University of Oslo

Criteria for Security Classification of Smart Home Energy Management Systems (long version)

Manish Shrestha , Christian Johansen , Josef Noll

Research report 492, July 2019

ISBN 978-82-7368-457-8
ISSN 0806-3036

Criteria for Security Classification of Smart Home Energy Management Systems (long version)

Manish Shrestha Christian Johansen Josef Noll

July 2019

Abstract

Internet of Things (IoT) is a growing field and its use in home automation is one of the dominating application areas. The heterogeneity and limited capacity of storage and processing power make the security of IoT systems challenging. Besides, the end users lack security awareness and 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 end users and for developers. Furthermore, regulatory bodies can use our security classification method as a reference to derive requirements for adequate security. This report presents a security classification methodology and extends it for the 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 is a good indication of the level of security, as well as a guide to improve the security of IoT systems.

This technical report is a long version of the conference paper [28].

[0] *Address for correspondence:*
Department of Informatics, University of Oslo, P.O. Box 1080 Blindern, 0316 Oslo, Norway.
E-mail: `cristi@ifi.uio.no`

Contents

1 Introduction

The proliferation of the Internet of Things (IoT) has created new transformative opportunities. One good example can be observed within smart homes [2, 31]. Aldrich defines the concept of *smart homes* as "a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security and entertainment through the management of technology within the home and connections to the world beyond" [2]. Today, the applications inside smart homes are more than luxury, where, e.g., energy management systems can enable efficient utilization of energy [14]. Modern smart home systems are composed of several sensors and actuators that communicate with a central hub called gateway, which might connect the sensor network to a cloud system.

Industrial IoT providers are usually driven by the development of functionalities, creating a range of communication and sensing capabilities integrated into small devices. However, from the customer's point of view, security and privacy has been a major concern, and often hinders a wider adoption of IoT systems. According to Symantec's Internet Security Threat Report (ISTR) 2018, the number of cyberattacks on IoT devices has increased by 600% between the years 2016 and 2017.[1] This is an indication that current security practices need to evolve to fit IoT systems, which is formed by the integration between several heterogeneous components.

This report is an exemplification and enhancement of our previous work [29] where we have introduced a general security classification methodology for smart grid systems and Advanced Metering Infrastructures (AMI). In this report, 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 from one of our partner companies E2U Systems AS. 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. We also describe the major communication standards used in SHEMS. 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. We consider two alternatives for device control mechanism for demand response activities and evaluate their class to illustrate the applicability of security class methodology. Section 5 concludes our work with an overview of future work.

2 A Commercial Home Energy Management System

This section provides a brief overview of typical smart home systems describing its components. Next, we take a real example of one of the smart home solution provided by Develco Products and describe its architecture and how such systems are being used to provide practical solutions in the industry. The main goal is to develop a certification scheme which can be used also internally within an IoT company to specify baseline security requirements and maintain the security level over time.

[1] Symantec Corporation, "Internet Security Threat Report(ISTR), Volume 23". https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

2.1 SHEMS Reference Architecture

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 [19,20,32]. Heat pumps are typical examples of load resources. Similarly, car batteries and solar panels are examples of storage and generation resources respectively. Functional modules of SHEMS may include monitoring, logging, control, management, or alarm services [32]. Ghirardello et al. [16] summarize a smart home reference architecture (see Fig. 1) by integrating three different viewpoints: (i) functional viewpoint, (ii) physical viewpoint, and (iii) communication viewpoint. The functional viewpoint focuses on the functionality of the IoT network in a smart home environment. Similarly, the physical viewpoint is concerned with the physical components involved to meet the functionality. The communication viewpoint focuses on the communication technology that enables interactions between the physical components. Thus, this framework gives an overview of the physical components and the interactions between them.

Based on this architecture, we describe the major components of smart home systems below.

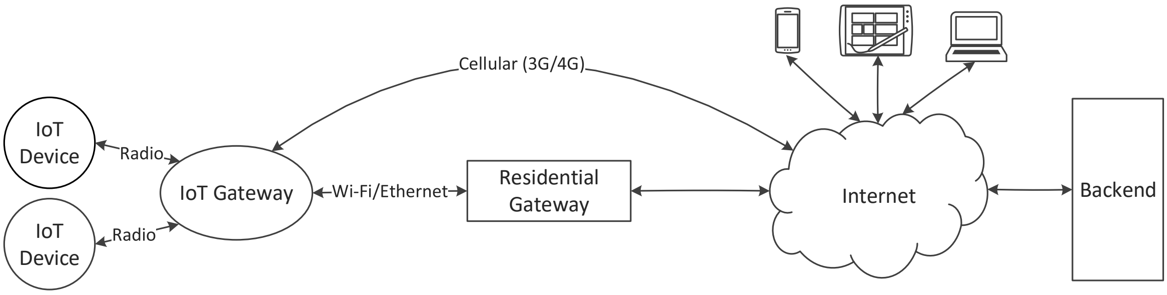

Figure 1: Smart Home System Architecture.

A SHEMS consists of IoT devices, IoT Hubs, residential gateways, clients (including smartphones, tablets, computers and software applications to utilize the services to the consumers), communication channels, backend systems, and Application and Network Data (AND). These components utilize wired or wireless communication channels to communicate with the cloud, as depicted in Figure 1.

IoT Devices. These have as primary functions [16] 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. Some examples of smart home devices include humidity sensors, heat alarms, motion sensors, meter interfaces, smoke detectors, window-sensors, thermostats, smart plugs and light dimmers.

IoT Hub. It acts as a central controller of IoT devices as well as a bridge between these and the backend system. Sensor data are reported to the IoT hub, which translates and sends them 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. The smart home gateway connects sensors and actuators to the backend system through the Internet. In other words, it is a bridge between the HAN and the Wide Area Networks (WAN). Quite often an IoT hub and residential gateway functionalities are integrated into one device.

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 such as Zigbee, Z-Wave, Wireless M-Bus, Thread [9,16]. 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.

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 [31].

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.

2.2 Major Communication Standards

Here we describe three major communication standards used in Commercial SHEMS for HAN.

2.2.1 Zigbee

Zigbee is a low-cost, lower-power consuming, two-way wireless communication standard from Zigbee Alliance. It enhances the IEEE 802.15.4 standard by using the Network layer and Application layer to define additional communication features. It uses the open trust model where each network layer in the protocol stack trusts each other. There are three types of nodes in a Zigbee network: coordinator, router, and end-device. A Zigbee network has only one coordinator and acts as a parent of all the nodes in the network. A coordinator allows other nodes to join the network by selecting an appropriate channel, frequency, and PAN id of the network. A router node is used to route traffic between different nodes. However, an end device does not route any traffic, as it simply sends or receives messages from a router or a coordinator.

Zigbee devices provide access control, data encryption, data integrity, and replay protection [11]. A Zigbee network supports three types of encryption keys: master key, network key, and the link key. A master key is generally used for exchanging link keys. Master keys are usually pre-installed, whereas some systems may have a key-load mechanism where a dedicate key-load key (derived from link key) is used to protect the master key during transport from the trust center to the device in the network. Zigbee uses AES (Advanced Encryption Standard) 128-bit encryption for exchanging messages.

To simplify the interoperability of devices, Zigbee provides, by design, the same security level for all devices in all the layers in the network [3]. Therefore, if there is one device in the network that does not support a higher level of security, then the security of the whole network is downgraded to a lower level of security. To overcome this issue, either critical devices should have a separate network or all devices in the network should support the required level of security. Table 1 shows security levels available for network and application layers in Zigbee.

Table 1: Security Levels in Zigbee Network and Application Layers [3]

Security Level Identifier	**Security Attributes**	**Data Encryption**	**Frame Integrity (length M of Message Integrity Code (MIC), in Number of Octets)**
0x00	None	OFF	NO (M=0)
0x01	MIC-32	OFF	YES(M=4)
0x02	MIC-64	OFF	YES(M=8)
0x03	MIC-128	OFF	YES(M=16)
0x04	ENC	ON	NO
0x05	ENC-MIC-32	ON	YES(M=4)
0x06	ENC-MIC-64	ON	YES(M=8)
0x07	ENC-MIC-128	ON	YES(M=16)

Though Zigbee offers strong encryption mechanisms, failing to protect the keys may result in security breaches [11]. Replay protection is based on the frame counter; if the latest counter is less than the last received counter, the message is ignored. An attacker could modify the message by increasing the counter [13] and then launch replay attacks. Proper key management, tamper resistance/detection and replay protection mechanisms can elevate security in Zigbee networks [12, 13, 33].

2.2.2 Z-Wave

Z-Wave is based on the G.9959 specification from ITU which specifies the Physical and MAC layer. Like Zigbee, it consumes little power and has long battery life. A Z-Wave network includes two types of nodes based on their roles: controller and slave. The controller sends commands to the slaves and is responsible to add or remove slaves from the network, having a full overview of the network. Slave nodes are the sensors and actuators that reply and execute the commands from the controller node. These are also capable of forwarding the commands to other nodes.

An open source implementation of Z-Wave called OpenZWave is available. It is based on public information and reverse engineering.[2] Currently, Z-Wave specifications are made available as a public standard at http://zwavepublic.com. Since most of the details of Z-Wave was not open until 2016, very few security assessments are publicly available.

Z-Wave uses AES 128-bit encryption for data security. It is backward compatible and is highly interoperable. The security framework "S2" of Z-Wave supports Diffie-Hellman key exchange, which makes the key exchange process more secure than in Zigbee. However, Z-Wave supports older devices that do not support encrypted and authenticated communications. This weakens the security of the Z-Wave network [1]. Moreover, one can also downgrade the security process to the previous version and exploit its vulnerabilities to compromise the network.[3]

The work of [15] found implementation issues of Z-Wave, where all 16 bytes of the temporary key used to exchange the encryption key were all zeros, which allowed to decrypt the encryption key. It was also observed that there was no state validation in the key exchange protocol. Therefore, the slave does not know if the key derivation has already been performed. Thus,

[2] "OpenZWave". https://github.com/OpenZWave/open-zwave.

[3] "Z-Shave. Exploiting Z-Wave downgrade attacks". https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/. . Accessed: October 26, 2018

one could spoof the controller and request a new key derivation process, which can reset the established network key on the target device and issue unauthorized commands to the slave devices.

2.2.3 Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) is a low-power, low-cost wireless protocol that supports frequency-hopping over 40 channels.[4] BLE also supports multiple network topologies. Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) is another version of Bluetooth that supports only point-to-point network topologies and is optimized for continuous data streaming. Since BLE is designed to be scalable for larger networks, it is suitable for home automation systems. BLE typically supports four association models:

- *Numeric Comparison*: In this model, the user is shown a 6-digit number on both displays and then asked to confirm whether the numbers are identical, thus protecting the network from MITM (man-in-the-middle) attacks.
- *Just Works*: This model also uses Numeric Comparison, but the user is never shown a number, and the application may accept the connection. This model is prone to MITM attacks.
- *Out of Band*: This model uses Out of Band mechanisms to discover the devices and exchange the keys for the pairing process.
- *Passkey Entry*: This model is used when one of the devices has the input capability but does not have a display. Then, the user will be displayed the 6-digit passkey in one device and ask another device to enter it.

BLE provides five basic security services, namely Authentication, Confidentiality, Authorization, Message Integrity and Pairing/Bonding [26]. BLE also preserves privacy by changing the device addresses frequently, making it difficult to track the devices on the network [9]. BLE supports two security modes, Mode 1 and Mode 2. Mode 1 has four levels of security:

1. No security (No authentication and no encryption)
2. Unauthenticated pairing with encryption
3. Authenticated pairing with encryption
4. Authenticated LE Secure Connections pairing with encryption using a 128-bit strength encryption key.

The higher level of security satisfies the lower levels. For example, level 2 security satisfies level 1, level 3 satisfies level 2, and so on.

Similarly, LE Security Mode 2 has two security levels:

1. Unauthenticated pairing with data signing
2. Authenticated pairing with data signing

Vendors could also select which security mode their devices will operate in and with what level within that mode. If vendors do not choose level three they will lose either data encryption, integrity, authentication or a combination of three.

[4] "Radio Versions". https://www.bluetooth.com/bluetooth-technology/radio-versions.

Security of BLE highly depends on the configuration selected for the system. Bluetooth 4.2 and onwards has support for Elliptic Curve Cryptography (ECC). However, ECC in legacy mode pairing is vulnerable to MITM [9]. As BLE was designed for star topology networks, data channels are protected only for a single hop. Hence, BLE does not support end-to-end encryption and authentication in mesh networks [10, 26]. Thus, additional security controls should be provided on top of the Bluetooth stack [26]. The work of [18] pointed out that the Temporary Key (TK) which is used to generate the encryption key can be brute-forced in less than 20 seconds because of its short length. Thus, they proposed to increase the length of TK to improve BLE security.

2.3 Comparisons

In Table 2 we compare the above three standards, which are meant to be used in home automation domain. In this table, for simplicity, we have not considered the configuration of the system for computing security classes and assumed that they have the best configuration. Otherwise, considering different configurations may result in a different table for different settings of security attributes. For instance, if the security level for Zigbee is set to level 4, then it will only have encryption but no frame protection mechanism, which will eventually degrade the protection level and will eventually affect the security class.

In our case, Z-Wave and BLE have a higher level of protection than Zigbee in terms of key exchange as they use asymmetric encryption, as opposed to symmetric encryption used in Zigbee. In the case of BLE, end-to-end encryption is not supported. However, it can be protected by using a star topology instead of a mesh network topology. Moreover, Z-Wave specifications are not completely open, which should also be taken into consideration when selecting the right technology. In our case, over the air upgrade is supported only for Zigbee and thus, though Zigbee does not support asymmetric encryption for key exchange, we select the Zigbee supported system for our case study.

Table 2: Comparison of major security functionalities in Zigbee, Z-Wave, and BLE.

Security Mechanism	**Protection Level**		
	Zigbee	**Z-Wave**	**BLE**
Data Encryption	Y	Y	Y
End-to-end Encryption	Y	Y	N
Node authentication	Y	Y	Y
Key exchange	Y (symmetric)	Y (asymmetric)	Y (asymmetric)
Integrity Protection	Y	Y	Y

2.4 System Description

As a case study, we apply our security classification to the commercial smart home solution offered by E2U Systems AS using hardware provided by Develco Products and implement customized software solutions for smart homes.[5] Develco Products[6] focuses on smart home and smart energy domain and delivers a wireless infrastructure platform for solution providers. In this section, we briefly describe the smart home solution provided by E2U Systems.

The Develco Products offer a Linux based IoT hub called *Squid.link gateway* (Fig. 2) consisting of ARM9TDMI, 454 MHz CPU (Central Processing Unit), and a variety of IoT

[5] "E2U Systems". https://e2usystems.com.

[6] https://www.develcoproducts.com

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, but 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 in the HAN network multiple wireless platforms, like Zigbee, Z-wave, Wireless M-Bus, Bluetooth Low Energy. We have considered Zigbee for HAN network during our analysis. The wireless module on the main board of the IoT gateway communicates with the CPU using the SmartAMM protocol, which is a proprietary protocol that also facilitates communications between gateways and the backend systems.

Before installing the smart home system into the households, it needs to be pre-configured, which includes registration of gateways and its devices in the backend system, so that a device can only communicate with the gateway to which it is registered. Unregistered or unknown devices cannot join the HAN network. Pre-configuration also involves the configuration of the gateway to communicate with the proper backend system.

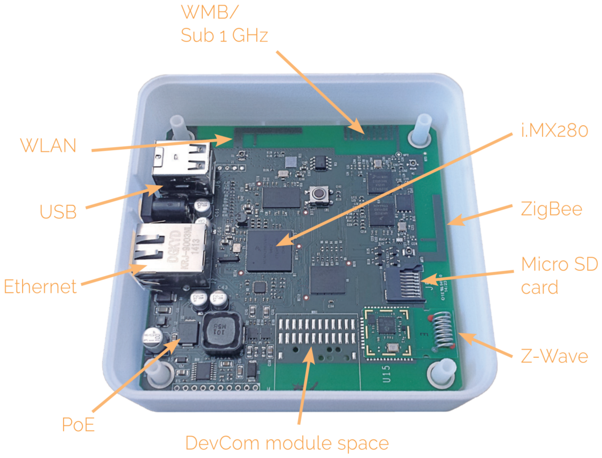

Figure 2: Squid.link Gateway

3 Extended Security Classification Method

The French "Agence Nationale de la Ssécurité des Systémes d'Information" (ANSSI) proposed a classification method for standardizing security measures for Industrial Control System (ICS) [4]. This classification is based on established risk analysis methods and provides general guidelines to determine the security class of an ICS. However, the computation of exposure in the ANSSI method does not fit smart grid systems, nor smart homes for the same matter. Therefore, we have proposed the Smart Grid Security Classification (SGSC) method [29], which extends the ANSSI classification method. 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 the connectivity surface). SGSC considers two major factors: Impact and Exposure. Impact indicates how critical a given subsystem is, whereas Exposure shows what functionality surface does it provide to be attacked.

Figure 3 summarises how a security class is computed. The computation first looks at the components of the system and then aggregates the results upwards until reaching the security classification of the whole. 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 point of view. The benefit is that the SGSC helps system designers to choose the most appropriate security functionalities to meet the envisaged security class. In addition, the focus on "secure-by-built" systems is better suited for long term applicability, as threats and vulnerabilities only represent a snapshot, whereas security classes present an inherent view of an IoT system.

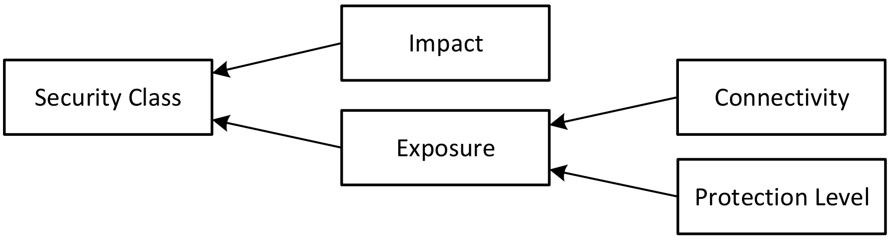

Figure 3: Methodology of computing a security class [29] (Impact as used by ANSSI).

In SGSC, we use five levels of impacts namely *Insignificant, Minor, Moderate, Major* and *Catastrophic*. Classifying impact is specific for the system under evaluation and is open to the judgement of security experts. We define exposure as the degree to which system's interfaces are available to attacks. There are two types of exposures: IT Exposure and Physical Exposure. Exposure is the result of Connectivity and Protection Level.

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.

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) [27]. SIL is the number assigned to the safety function of a given system.[7,8] SIL broke the belief that the safety of a system is binary and is either safe or not. It introduced *levels* for safety [27]. Using a similar approach, Security Levels were introduced in the ISA-99 standard, which later changed to Security Assurance Levels (SALs). SAL is influenced by SIL but the levels of SAL are based on the strength of attackers. Because security systems have much broader application, consequences and possible circumstances, [17] claim that representing security assurance level by a mere number is not enough, and therefore, propose a vector approach to describe security requirements.

We use a similar approach as SAL by introducing Protection Category (PC). However, instead of the attacker model, we consider the connectivity of the system when setting the required security mechanisms. We have defined five levels of protection categories to represent the increasing scope of security functionality, which is as follows [29]:

[7] "SIL Made Simple". http://www.valve-world.net/pdf/vw10ce_actuation_-cameron.pdf

[8] "Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications". Schneider Electric white paper.

PC 1: Includes Physical and Environmental Protection

PC 2: Includes PC 1 and Network Protection

PC 3: Includes PC 2 and Wireless Protection

PC 4: Includes PC 3 and Private Infrastructures protection

PC 5: Includes PC 4 and Cloud protection

PC represents the goal of protecting a given type of setup by using security functionalities (or 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. Below are the guidelines to determine the protection levels:

Protection Level 1 (P1) : This level includes systems that have no security mechanisms.

Protection Level 2 (P2) : This level possesses basic security features and has little impact on improving security. Security functionalities implemented are easy to break, e.g., WEP (Wired Equivalent Privacy) password.

Protection Level 3 (P3) : This level of protection provides advanced security concepts, e.g., WPA (Wireless Protected Access) passwords.

Protection Level 4 (P4) : Protection level 4 possesses advanced security concepts, including also basic monitoring capabilities.

Protection Level 5 (P5) : This level possesses state-of-the-art protection mechanisms and advanced monitoring capabilities. Additionally, there are no vulnerabilities and issues discovered in any of the component or security mechanism. If a new security issue is discovered in a system/subsystem/component, it can no longer have protection P5. It will rather degrade to lower levels.

Table 3 shows the evaluation of exposure level from connectivity and protection level. The evaluation of the protection level is conducted by security experts.

Table 3: Calculation of Exposure Levels

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

A security class can be expressed in terms of impact and exposure levels. A security class represents the quality of security of a given system and is represented by letters A to F, where A represents the highest security class and F being the lowest. A higher security class means either the impact is low, or the exposure is low. If the impact is high, the exposure must be reduced to obtain a higher class. Thus, a security class can be improved by lowering either exposure or impact, or both (see table 4). Security classes can be used not only for determining the security status of the system, but also to define the appropriate security requirements for a given system. Thus, it can be used to make purchase decisions on smart home systems for residents and also for regulatory bodies to have control over the security standard of IoT systems.

Table 4: Calculation of Security Classes

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

In our earlier work, we have not considered protection mechanisms in detail (the same as how standards like ANSSI also do) [29]. In this report, we detail this important part of our SGSC by ranking various security functionalities, focusing on our smart home application domain. Table 5 lists classes of functionalities and their respective sources.

Table 5: 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

The goal of this research is to help industries establish and maintain good security standards of their systems by providing guidelines and strategies to improve overall system security. Understanding the sources of threat and the impacts is one way to understand the criticality of the system [6]. For instance, control command on an autonomous vehicle is much more critical than the control command to switch off the lights of a bedroom. We extend [29] by extracting the security criteria for evaluating protection levels based on the following standards and best practices:

ISO 27002 This standard provides general guidelines on information security management. Like other standards, it is also highly document-oriented. However, it does not cover the IoT systems until now [9].

Cloud Security Alliance (CSA) The IoT Working Group of CSA provides 13 step guidelines and considerations to secure IoT products targeted towards the developers of IoT devices [10].

[9] ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls (second edition).

[10] IoT Working Group, Cloud Security Alliance (CSA), "Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products". https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Industrial Internet of Things (IIC) The Industrial Internet of Things Volume G4 Security Framework provides the Business and Functional viewpoints towards IoT security [11]. It describes the architecture of IoT systems and provides guidance to create secure IoT systems.

OWASP "IoT Security Guidance" provides general guidelines to the manufacturers, developers, and consumers to secure their IoT products [12].

ETSI TS 103 645 is a technical specification entitled "Cyber Security for Consumer Internet of Things" that provides cybersecurity guidelines for entities manufacturing and developing consumer IoT solutions.[13]. This ETSI technical document is based on the UK government's document for the Code of Practice for Consumer IoT Security.[14]

Below we describe the security criteria synthesized for SHEMS from the above sources:

Data Encryption Data should always be encrypted during transport. If sensitive data are stored in the device, they should also be adequately encrypted. When implementing encryption mechanisms, proprietary protocols should be avoided. It should be ensured that SSL/TLS implementations have proper configurations and are up to date [7].

Communication and Connectivity Protection Communication channels between components can be protected by protecting information flow and endpoints. Endpoints have different capabilities and security requirements. This may include mechanisms like network data isolation, network segmentation, firewalls, unidirectional gateways, network access control, etc.[10]

Software/Firmware Security The firmware software is the core of a component. Unauthorized modification of software may result in security threats. Therefore, it should be ensured that software/firmware are protected against unintended and unauthorized updates and modifications. Update Servers (i.e., servers responsible for sending system/firmware updates to the system components) must be trusted and in a secure state so that no illegal software can be sent out as updates. For classical IT systems, examples include the Windows Server responsible for handling updates for other computers in the corporate network, whereas for IoT infrastructures an update server could be responsible for over the air updates like the Zigbee OTA Upgrade Cluster.

Signing update files and validating on the devices before installation may protect illegal installation and updates. If possible, software and firmware should be updated as soon as vulnerabilities are discovered and fixes are available. There should also be the provision to implement scheduled updates. Also, the update process of firmware should take care of unwanted situations like network and power disruptions [22].

Hardware-based Security Controls Hardware protection should go along with the software protection. Software weaknesses and misconfigurations are not the only sources of attacks in the IoT world. One of the factors on which hardware security depends is the security of the micro-controller used in a given device. It also depends on whether a Trusted Platform Module (TPM) is integrated into the component, and how it is used [5, 8]. There are other mechanisms like using Memory Protection Units, incorporating Physically Unclonable Function

[11] Industrial Internet Consortium, "Industrial Internet of Things Volume G4: Security Framework". https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[12] OWASP, "IoT Security Guidance". https://www.owasp.org/index.php/IoT_Security_Guidance

[13] ETSI TS 103 645, https://www.etsi.org/deliver/etsi_ts/103600_-103699/103645/01.01.01_60/ts_103645v010101p.pdf

[14] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

(PUF), using cryptographic modules, etc., that may contribute to hardware protection of the system [21,25].

Access Control Access control refers to mechanisms for protecting assets from unauthorized components, based on the business and security requirements (cf. ISO 27001). Access control can be achieved through authentication and authorization mechanisms which validate the interacting components and their privileges against system access.

Cryptographic Techniques There are two types of cryptography namely symmetric and asymmetric cryptography. In symmetric cryptographic techniques, the parties exchanging information share the secret key which is used for encrypting and decrypting messages. Whereas in asymmetric cryptography, one party distributes its public key to other parties who use these to encrypt the message, which can only be decrypted using the private key, which is kept secret. Cryptographic techniques are basically used to ensure confidentiality. These techniques can be implemented for protecting communication and connectivity and establishing secure key management. Examples of its applications useful for IoT and smart grid are message authentication, protected key store, code signing, secure bootstrapping, secure patch management and mutual authentication.[10]

Physical and Environmental Security The system components should be protected against unauthorized physical access. This criterion evaluates how well the system is protected against physical access and environmental conditions. Depending on the context, it may include access control of physical perimeter (area, building, home, room, etc.,) and set of equipment [10]. In the case of equipment, it may have several physical ports accessible that can be misused. Protection mechanisms like disabling unused physical ports or installing equipment with minimal physical ports, physical tamper detection, etc., fall under this criteria [12].

Logging and Monitoring Logging and monitoring help tracking and analyzing activities going on in the system. In case of security incidents, monitored processes and logged data may help to understand the cause and prevent such incidents from happening again. Systems like Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) help to identify and prevent attacks on the system and its components. Thus, evaluating the logging and monitoring mechanisms used by a system is an important security criterion for security classification.

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 [15]. We utilize the security functionality from this framework to fit our need to specify protection levels. Table 6 shows the mapping of security criteria to security functionalities and protection level.

4 Applying the Extended Security Classification to SHEMS

The SHEMS in our case complies with the reference architecture from Section 2.1 and consists of a centralized IoT hub and smart plugs connected to controllable loads such as water heater, air conditioner and floor heating. For simplicity, we do not include storage devices such as batteries that can act as both load and generation device.

[15] https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

Table 6: 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			

4.1 Impacts

Below we 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 a burglary or other types of crime. Moreover, residents may feel unsafe (reducing trust in SHEMS) if they realize that their privacy is breached and strangers can follow their activities.

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 [23,30].

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

Privacy. Data from SHEMS can be privacy sensitive, as Molina Markham et al. have demonstrated that High-frequency consumption data can be exploited to derive private information such as the number of people in the house, sleep routines, and the presence of babies at home [24]. Compromised SHEMS data may contain even more detailed information. Stealing such data may result in the exposure of personal habits of the residents, which can 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.

4.2 Protection Level for security criteria

Each security criterion demands several security functionalities, adequately configured, in order to reach a given protection level. Here we describe the security functionalities of our system to determine the protection level.

Data Encryption The IoT hub utilizes TLS so that the communication between the IoT hub and the backend system is always encrypted. IoT devices and IoT hubs form a HAN communicating Zigbee. In addition to AES 128-bit encryption, Zigbee also supports end-to-end encryption which is typically safe for mesh networks.

Communication and Connectivity Protection Typical households have a single Local Area Network (LAN). Therefore, if the gateway is connected via Wi-Fi or Ethernet, it forms one of the nodes in the LAN. If an attacker has access to the Wi-Fi network, then the smart home gateway becomes accessible. However, remote access has key-based authentication which reduces the gateway's exposure. Similarly, nodes also have pre-distributed keys, and only authorized nodes can join the radio network.

Software and Firmware Security The capability of a networked system of being upgraded is important for IoT systems. Develco Products smart home system provides the possibility to update the system devices and applications. The operating system is upgraded using SSH which only supports key-based authentication. Data flowing during a system upgrade is also encrypted. Similarly, for firmware upgrades of Zigbee modules, a Zigbee OTA Upgrade Cluster server is implemented. The upgrade process provides security via image verification, authentication, and encryption as specified in Zigbee OTA Upgrade Cluster specification.

Hardware-based Security Controls In this work we have not looked into hardware-based security controls and thus is not applicable.

Access Control Only authenticated IoT devices can join the HAN with the IoT Hub. All devices including the IoT gateway have pre-shared keys which allow them to communicate with each other through encrypted channels. E2U systems use Microsoft IoT hub for communication and management of SHEMS over the cloud. Microsoft IoT hub provides multiple ways to secure communication including token-based and certificate-based authentication mechanisms.[16] Only registered and active IoT hubs(gateways) can communicate with the backend system. End users can only access authorized devices. Administrators have control over the management of smart home gateway systems. Microsoft IoT hub also allows remote monitoring of smart home systems. The security of a smart home system also depends on the security of the backend system. Since we have excluded the backend system and assumed it to be secured, the available access control features are adequate.

Cryptographic techniques The IoT hub and IoT devices are pre-configured and use installation codes, certificates, and pre-defined keys to authenticate the connection. This means that only registered and pre-configured smart home devices can join its assigned gateway. The radio communication uses Zigbee, and data is encrypted using AES 128-bit key. Symmetric link keys (i.e., a unique key for each established link in the network) are used to encrypt data between the gateway and the devices in the network. Similarly, Wi-Fi supports WPA2-PSK (AES/TKIP) encryption. Data integrity is supported by using MIC (Message Integrity Code).

Physical and Environmental Security The system that we have considered has no tamper detection mechanisms for physical security. However, the components of SHEMS are located inside the house and unauthorized users have no physical access to the system.

Monitoring and Analysis The advanced monitoring capabilities include the collection of security data from system components, analysis and taking necessary actions if required based on the analysis. Smart home systems support basic monitoring functionalities where data log information is collected from the devices and sent to the backend. The gateway performs availability checks on its devices and reports to the backend system, but it does not perform extensive security analysis.

Based on our protection level requirements (see Table 6), the protection level of our SHEMS is set to P4.

4.3 Evaluation of Security Class

We limit the presentation of the application of security classification only to Application and Network Data. In particular, we assess the Command and Control (C&C) for a demand re-

[16] Control access to IoT Hub, https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-security.

sponse program, which is one of the most critical components of SHEMS. We apply the classification method for the following two scenarios.

4.3.1 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. Depending on the device and their maximum effect, rules for controlling the devices 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 a minimum of 15 minutes. The DSOs forecast the energy demand in advance and, if reductions are needed, DSOs optimally select the devices to be turned off. Such an operation meets the goal of reducing energy. Control commands are sent to the selected devices from the DSO to meet the goal of targeted reduction of consumption. The state of all affected devices may be reverted back to their original state after the duration of the demand response execution is complete.

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 earlier. 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. Using Table 6 and sub-section 4.3, we assign the overall protection level P4.

Using Table 3 we determine from the computed values of connectivity (C5) and protection level (P4), the exposure E3. Using Table 4 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 4 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 3.

4.3.2 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, allowing control of 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 3(a), we obtain the Exposure E2 and using Table 4 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. Besides, 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

In this report, we discuss the architecture of a commercial smart home energy management systems. We also compared three major communication standards for home automation network to discuss their security features. We present the security classification methodology extended with details regarding security functionalities relevant for SHEMS. As an example, we have applied this methodology to the commercial SHEMS from E2U. The example focusses on the C&C part of SHEMS for demand response programs. We have first evaluated the security class of the C&C for a centralized control architecture, resulting in a low and unacceptable security class D. Using our methodology, we can indicate how the system needs to be improved to achieve an acceptable security class. Using an edge controlling concept, our analysis demonstrated an achievable security class A. Further work will focus on aggregation mechanisms for calculating the overall system security class from its components.

References

[1] Giovanni Agosta, Alessio Antonini, Alessandro Barenghi, Dario Galeri, and Gerardo Pelosi. Cyber-security analysis and evaluation for smart home management solutions. In *Security Technology (ICCST), 2015 International Carnahan Conference on*, pages 1–6. IEEE, 2015.

[2] Frances K Aldrich. Smart homes: past, present and future. In *Inside the smart home*, pages 17–39. Springer, 2003.

[3] ZigBee Alliance. Zigbee specification. 2012.

[4] ANSSI. Classification Method and Key Measures. 2014.

[5] Will Arthur and David Challener. *A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security.* Apress, 2015.

[6] Ahmad W Atamli and Andrew Martin. Threat-based security analysis for the internet of things. In *2014 International Workshop on Secure Internet of Things*, pages 35–43. IEEE, 2014.

[7] Michael Atighetchi, Nathaniel Soule, Partha Pal, Joseph Loyall, Asher Sinclair, and Robert Grant. Safe configuration of tls connections. In *Communications and Network Security (CNS), 2013 IEEE Conference on*, pages 415–422. IEEE, 2013.

[8] Sergiu Bursuc, Christian Johansen, and Shiwei Xu. Automated Verification of Dynamic Root of Trust Protocols. In Matteo Maffei and Mark Ryan, editors, *6th International Conference on Principles of Security and Trust (POST)*, volume 10204 of *Lecture Notes in Computer Science*, pages 95–116. Springer, 2017.

[9] Daniel Celebucki, Maj Alan Lin, and Scott Graham. A security evaluation of popular internet of things protocols for manufacturers. In *ICCE*, pages 1–6. IEEE, 2018.

[10] Seyed Mahdi Darroudi and Carles Gomez. Bluetooth low energy mesh networks: A survey. *Sensors*, 17(7):1467, 2017.

[11] Bo Fan. Analysis on the security architecture of zigbee based on ieee 802.15. 4. In *Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on*, pages 241–246. IEEE, 2017.

[12] Xueqi Fan, Fransisca Susan, William Long, and Shangyan Li. Security analysis of zigbee. 2017.

[13] Fadi Farha and Hongsong Chen. Mitigating replay attacks with zigbee solutions. *Network Security*, 2018(1):13–19, 2018.

[14] Puteri Fitriaty, Zhenjiang Shen, and Kenichi Sugihara. 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*, pages 39–76. Springer, 2018.

[15] Behrang Fouladi and Sahand Ghanoun. Security evaluation of the z-wave wireless protocol. *Black hat USA*, 24:1–2, 2013.

[16] K Ghirardello, C Maple, D Ng, and P Kearney. Cyber security of smart homes: Development of a reference architecture for attack surface analysis. 2018.

[17] James D Gilsinn and Ragnar Schierholz. Security assurance levels: a vector approach to describing security requirements. In *Proceedings of the US DHS industrial control systems joint working group (ICSJWG) 2010 Fall Conference, Seattle, USA*, 2010.

[18] Giwon Kwon, Jeehyeong Kim, Jaewon Noh, and Sunghyun Cho. Bluetooth low energy security vulnerability and improvement method. In *Consumer Electronics-Asia (ICCE-Asia), IEEE International Conference on*, pages 1–4. IEEE, 2016.

[19] Jeong In Lee, Chang-Sic Choi, Wan-Ki Park, Jin-Soo Han, and Il-Woo Lee. A study on the use cases of the smart grid home energy management. In *ICTC*, pages 746–750. IEEE, 2011.

[20] Yuanyuan Liu, Bo Qiu, Xiaodong Fan, Haijing Zhu, and Bochong Han. Review of smart home energy management systems. *Energy Procedia*, 104:504–508, 2016.

[21] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security*, pages 3–37. Springer, 2010.

[22] H. Mansor, K. Markantonakis, R. N. Akram, and K. Mayes. Don't brick your car: Firmware confidentiality and rollback for vehicles. In *2015 10th International Conference on Availability, Reliability and Security*, pages 139–148, Aug 2015.

[23] Amir-Hamed Mohsenian-Rad and Alberto Leon-Garcia. Distributed internet-based load altering attacks against smart power grids. *IEEE Trans. Smart Grid*, 2(4):667–674, 2011.

[24] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. Private memoirs of a smart meter. In *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, pages 61–66. ACM, 2010.

[25] Thomas Morris. Trusted platform module. In *Encyclopedia of cryptography and security*, pages 1332–1335. Springer, 2011.

[26] John Padgette. Guide to bluetooth security. *NIST Special Publication*, 800:121, 2017.

[27] Felix Redmill. Understanding the use, misuse and abuse of safety integrity levels. In *8^{th} Safety-critical Systems Symposium*, pages 8–10, 2000.

[28] Manish Shrestha, Christian Johansen, and Josef Noll. Criteria for Security Classification of Smart Home Energy Management Systems. In *1^{st} International Conference on Smart Information and Communication Technologies*, Lecture Notes in Electrical Engineering. Springer, 2019. (to appear).

[29] Manish Shrestha, Christian Johansen, Josef Noll, and Davide Roverso. A Methodology for Security Classification applied to Smart Grid Infrastructures. *International Journal of Critical Infrastructure Protection (IJCIP)*, 2019. (to appear).

[30] Saleh Soltan, Prateek Mittal, and H Vincent Poor. Blackiot: Iot botnet of high wattage devices can disrupt the power grid. In *27th USENIX Security Symposium*, pages 15–32, 2018.

[31] Biljana L Risteska Stojkoska and Kire V Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140:1454–1464, 2017.

[32] Bin Zhou, Wentao Li, Ka Wing Chan, Yijia Cao, Yonghong Kuang, Xi Liu, and Xiong Wang. Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renewable and Sustainable Energy Reviews*, 61:30–40, 2016.

[33] Tobias Zillner and S Strobl. Zigbee exploited: The good the bad and the ugly. *Black Hat–2015 https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf*, 2015.