Security Requirements for Managing Smart Objects in Home Automation

Stefanie Gerdes and Olaf Bergmann

Universität Bremen, Bremen, Germany
{gerdes,bergmann}@tzi.org

Abstract. Enabling technologies for the Internet of Things are well understood, and open standards exist that define how to use the Internet Protocol, Version 6, (IPv6) to interconnect smart objects with each other and to the public Internet. As these devices typically are quite limited in their hardware resources, security is often considered too expensive and is sacrificed for a marginal extension of battery lifetime. Missing security not only exposes the application logic to evildoers but also affects management functions. In this paper, we discuss potential threats to machine-to-machine communication and provide a detailed example how protection requirements can be inferred from a given application scenario.

Keywords: wireless sensor networks, 6LoWPAN, constrained devices, light-weight security, protection requirements, impact analysis.

1 Introduction

The Internet of Things (IoT) today is regarded as an integral part of the future Internet [1]. With IEEE 802.15.4 and 6LoWPAN [2] as enabling technologies, hardware manufacturers as well as software developers envision the Internet Protocol, Version 6, (IPv6, [3]) to become the standard communication protocol for interconnecting smart objects. This trend also has leveraged the replacement of proprietary protocol stacks for machine-to-machine (M2M) communication by standardized and open architectures that use IPv6 for data transport [4].

Exposing smart objects to the Internet also makes them vulnerable to various threats that do not exist or are at least ignored for isolated networks. While proven security protocols exist to defeat many of these attacks in the "old" Internet, the IoT has many inhabitants that have only limited capabilities in terms of processing power, available memory, and means for user interaction. Moreover, these devices often are battery-powered and thus are designed to consume very low energy during operation. Strong cryptography then would possibly render too expensive for most applications.

To provide a reasonable amount of security while still allowing device lifetimes of several years, light-weight security profiles for embedded devices are discussed in academia and standardization organizations (cf. Section 1.1). To trade the cost off against the achieved security level, it is required to examine

A. Timm-Giel et al. (Eds.): MONAMI 2012, LNICST 58, pp. 231–243, 2013.

the actual application thoroughly. In this paper, we show how this can be done by conducting a protection requirement analysis for a simple home automation scenario.

The paper is structured as follows: The remainder of this section gives some more background on security architectures for wireless sensor networks and the Internet of Things, followed by a short introduction of the application scenario that is used throughout the rest of this paper. Section 2 explains the categories of information that have been identified within the system. Section 3 then introduces the protection requirement categories and applies them to the individual types of information. The results of our analysis and their applicability for smart object design are discussed in Section 4. Section 5 then concludes this paper with a brief summary and a critical acclaim of our results.

1.1 Background

IoT-applications usually involve not only devices with limited resources but also challenging network capabilities such as small frame sizes, low bandwidth, and high variations of packet loss and transmission latency [5]. While some protocols such as the Simple Network Management Protocol (SNMP, [6]) can be used in these environments without any change, most protocols have initially been designed for a wired Internet with static hosts and less frequent route changes. Thus, new protocols have been developed to better deal with these deficiencies. One example is the Constrained Application Protocol (CoAP, [7]) that is intended to facilitate development of applications for the IoT.

Communication protocols for home automation systems have been discussed in [8]. The authors state that IPv6 and 6LoWPAN are well-suited for M2M-communication in home automation systems, with good solutions for security still missing. Both, CoAP and SNMPv3 rely on the underlying transport layer to provide a secure communication channel [7,9]. Datagram Layer Security (DTLS, [10]) currently is being regarded as the most viable solution to provide security for these two protocols.

Security threats on wireless sensor networks have been extensively discussed recently [11], and a concise classification of attacks is given in [12]. Overviews of light-weight security technologies for use with limited resources are presented in [13] and [14]. These publications focus either on attacks or on the solution space. We consider another approach useful for constrained devices: If detailed knowledge about the protection requirements of the various kinds of data in the system can be gained, it is possible to adapt the security concept accordingly. Security mechanisms can be explicitly chosen to meet the protection requirements and only mechanisms which are really needed in the scenario can be used. Thus the usage of resources like storage space, computing power and bandwidth can be reduced.

1.2 Scenario

In this paper, we discuss the protection requirements for automated light control in a "smart home". For simplicity, the scenario spans only two rooms, each of which is equipped with a group of lights. Each group has multiple lights controlled by a microcontroller to modify the illumination level. Light sensors are used to regulate the (electric) lights in a room according to the current daylight level. A main switch for the entire appliance provides three modes: "off", "on", and "automatic". In automatic mode, the available sensors can be used to achieve a certain illumination level. The more the daylight diminishes in the room, the more the brightness of the electric lights will increase.

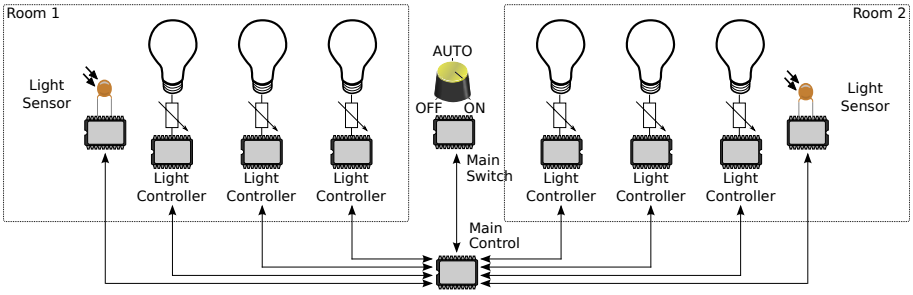

Fig. 1. System architecture with centralized main switch and separate rooms

The lights in a group are synchronized, i. e. they always have the same brightness value. All groups can be switched on or off at once using the main switch. Each group can have additional logic controls that maintain global state information for that particular group. State information is distributed in the network using multicast. Devices register at the main controller to get multicast messages for their group.

The scenario is based on an average private household. One or more occupants are living in the house who sometimes have visitors. Illumination in one or more rooms of the house is controlled by a constrained network using the architecture described above.

2 Data Categories

Communication within this network requires various types of information that can be divided in three main categories: State information of resources, configuration data and keying information for the cryptographic mechanisms.

Resources in this scenario are light bulbs, switches and sensors. The relevant state information of the switch is its position, whereas the light sensors' state information contains their measurements. Switch position and sensor values determine the state of the light bulbs, i. e. their illumination level. The main

controller calculates the desired light bulb state and then sets this state using a control message. The state information can be retrieved from a light bulb as well to update e. g. a user interface.

The following list summarizes the data in the system:

- State information of resources
  - Switch position (on, off, auto)
  - Sensor data values (in lux)
  - Light bulb state (in percent)
- Type of resource (switch, sensor, light bulb, controller)
- Configuration data
  - Transport address of group
  - Transport address of main controller
  - Physical location of resource (optional)
- Cryptographic keying material

The configuration data is necessary for proper operation of the node and for communicating within the network, including gateway addresses, multicast groups to listen on and human readable node identifiers. Nodes (sensors as well as light bulbs) are assigned to groups in order to control several nodes at once as shown in the initial scenario description (see Section 1.2).

Each group has its own transport address to enable communication within a group, e. g. to distribute state updates of a light sensor that belongs to that specific group. Additionally, all groups are controlled by a main controller which coordinates the nodes. It gathers the information from the sensors and calculates the values the light bulbs have to apply. The controlling node has to be replaceable in order to circumvent the breakdown of the whole group if the controller stops operating. Therefore, another node can take over operation. The current controller is identified by the controller's transport address recorded in the configuration data. As additional information for the user, the configuration data can optionally contain the physical location of the resource.

Finally, cryptographic keying material is needed to protect the communication within the network. This data is part of the protection mechanism which has to be applied to the system and as such has to be considered within the analysis of the protection requirements.

3 Classification of Protection Requirements

The Bundesamt für Sicherheit in der Informationstechnik (BSI) defines three protection requirement categories which range from *normal* and *high* to *very high* [15]. These values indicate the severity of damage that might be caused by security breaches. A similar approach is used by the National Institute of Standards and Technology (NIST) [16]. They define the three categories *low*, *medium* and *high* to evaluate the magnitude of impact.

Both standards propose to classify the impact of compromising the main security objectives confidentiality, integrity and availability based upon these

categories. The separation between the categories is facilitated by the definition of damage scenarios which include law violations, impairment of the right to informational self-determination, physical injury, impaired abilities to perform tasks, negative internal or external effects and financial consequences.

For our home automation scenario, we define the protection requirement categories (PRCs) as follows: Breaches with no or only minor effects are assigned to the category *normal*. The category *high* includes more severe vulnerabilities, which can cause, e. g., physical injuries or heightened financial losses or violate significantly someone's privacy. Only vulnerabilites which might have very serious consequences belong to the category *very high*, e. g. where danger for life and limb is possible or where financial losses are so severe that they can ruin the affected person or organization.

These protection requirement categories are used below to classify the impact of security breaches for each of the identified data types (see Section 2). To provide more details, the main security objectives confidentiality, integrity and availability are analyzed separately.

3.1 State Information

To allow for light control at all, the states of the resources have to be transmitted. For example, the main controller has to be informed about the switch position and the sensor values.

Generally, state information makes it possible to detect when devices are activated. This knowledge might be used to create a behavioural profile, e. g. of the times an occupant is at home or how often she uses one of her rooms. This can seriously affect her privacy. Thus the confidentiality of the state information is considered to belong to the PRC high.

The integrity of state information is also very important. If the data is manipulated, a light bulb can be turned off although it is supposed to be on. At worst, a person in the house might be injured when trying to find a switch or a flashlight in the dark. For example, she might trip over some object and fall down. Security breaches which might cause an unauthorized deactivation of the light bulbs are always high because they might lead to physical injuries. Accordingly, the integrity of the state information data has PRC high.

If no state information is available within the system, the lights keep their current state. This behaviour can lead to physical injury if the lights cannot be turned on. As already mentioned, this is correlated to the PRC high. If the lights cannot be turned off, this leads to financial losings for the owner. As we only consider light control in our analysis, the losings will likely remain minor and belong to PRC normal. The sum of these two aspects result in the state information's availability to fall into the PRC high.

Switch Position. The switch position is the most important state information, because it can directly control the lights and override the data of the light sensors. The confidentiality of the switch position is considered to be PRC high, because

the occupant will likely turn off the lights when she is not at home. Thus her privacy is endangered by confidentiality breaches which leads to PRC high.

The light bulbs are directly controlled by the switch position. If it can be manipulated, the light bulbs can be turned off without permission. Thus, the integrity of switch state is also PRC high.

For similar reasons, the availability of the switch position has to be categorized as high as well. If it is impossible to control the light with the switch, the user has no direct control over the lights and therefore cannot turn it on or off. This might cause her to have to move around in the dark which endangers her physical integrity.

Light Sensor Values. The values of the light sensors seem less important, but still have serious impact. As the light sensors are applied to the room in order to measure the illumination level, they can be used to determine whether the light in a room is turned on or off. Like the switch position this information might endanger the privacy of the occupant. Thus, the light sensor values' confidentiality also belongs to the PRC high.

The integrity of this data is very important as well. The light bulbs can be directly regulated by them, at least as long as the switch is not used to control the light. If the light is turned off while no switch is within reach of the occupant, she might get hurt while trying to get there. Accordingly, the PRC of the integrity is high.

Availability is no issue in this case. If the light sensors fail, the light can still be operated with the switch. The PRC of the light sensor values' availability is therefore normal.

Light Bulb State. The importance of the light bulb state depends on the devices which are influenced thereof. As already mentioned, the main controller calculates the illumination level and sends it to the light bulbs. Therefore, the controller's light bulb state to-be is more important than the state of the single light bulbs.

Like the switch position, the state of the light bulbs might reveal details about the habits of the occupant. It therefore also has the PRC high. The modification of the light bulb state might cause one or, if the light bulb state sent by the controller is concerned, several lamps to be set to a certain state. They might be turned off or stay off although they should not. The integrity of the light bulb state therefore belongs to the PRC high. The availability of the light bulb state is only important for the light controller, because it tells the other lamps their status. Thus, the availability of the light bulb state is PRC normal while the availability of the controller's light bulb state is PRC high.

The classification of protection requirements for the state information is summarized in Table 1.

3.2 Resource Type

Confidentiality breaches in home scenarios can disclose personal information about the occupants. The type of the device reveals which devices are used

Table 1. Protection requirement classification: state information

Information	Confidentiality	Integrity	Availablity
State information	high	high	high
– Switch position	high	high	high
– Sensor data	normal	high	normal
– Light bulb state	high	high	normal
– Light bulb state of controller	high	high	high

within the house. This might be dangerous if thereby the existence of valuable items can be derived. For our home automation scenario only light control is considered. The according devices are assumed to be not particularly valuable. Thus, the confidentiality of the resource type is correlated to the protection requirement category normal.

Manipulating the integrity of the resource type might have a more serious impact. A node which wants to use the node's services might be mislead by a wrong or unreadable resource type. Thus, the sensor data might not be interpretable at all which results in the unavailability of the sensor data. The PRC of the resource type's integrity therefore is high, because it is at least as high as the category of the sensor data's availability. Additionally, if a device can be deluded to believe that a resource has a different type it might misinterpret the resource values. This might e. g. result in turning the lights off although they should be on, potentially leading to physical injuries. The classification therefore is high.

The availability of the resource type has the same protection requirement category as the integrity. If the resource type is not available the data might as well not be interpretable and hence cause failures. This means, the PRC of the resource type's availability is high as shown in Table 2.

Table 2. Protection requirement classification: resource type

Information	Confidentiality	Integrity	Availablity
Type of resource	normal	high	high

3.3 Configuration Data

The configuration data consists of information needed for the proper operation of the node and the communication within the network (see also Section 2).

Transport Address of Group. The disclosure of the transport address is not assumed to cause significant damage. No personal information can be derived from this information. The confidentiality of the transport address therefore has PRC normal.

A change of the transport address may cause the nodes to listen and send on a non-existing address and thereby lead to a failure of one or more nodes.

This might lead to unavailable state information and thus has at least the same PRC, which is high. Moreover, nodes may listen or send on the transport address of the wrong group. The results of this behaviour are difficult to predict. Although the consequences will in most cases be less severe it might still be possible that an occupant suddenly finds herself surrounded by darkness. All in all, the PRC of the group's transport address is high.

If the transport address of the group is not available to a single or several nodes, this might cause these nodes to fail. They can not send or receive messages any more and thus will keep their last state. Therefore the availability of this data belongs to the category high.

Transport Address of Controller. The confidentiality of the controller's transport address is not significant and therefore has PRC normal.

The Manipulation of the transport address would cause the light bulbs in the group to send their subscriptions to the wrong address which leads to wrong or missing state information. This equals the effects of integrity breaches of the group's transport address and has the same PRC (high). Additionally, the controlling node may be lead to believe another device to be the controller in which case he is not responsible for the distribution of state information to the light bulbs. This will cause all the light bulbs in the group to keep their last state. This is considered to be potentially harmful because the occupants might not be able to turn on the lights. The PRC is high in this case. According to these problems, the integrity of the controller's transport address is categorized as high.

Without the controller's transport address the nodes cannot register or refresh their registration. Eventually, they will not get any more status updates from the main controller and thus keep their last state. The availability is therefore PRC high.

Physical Location of the Node. The physical location of the node is very important for the user, because it helps him identifying the devices. Analyzing this data might reveal additional information about the occupants' living conditions. However, confidentiality breaches do not have a significant effect on the social or financial well-being of a person and thus fall into the protection requirement category normal.

Breaching the integrity by e. g. altering the node's location can mislead the user and delude him to assign the node to a wrong group. Thus a single, or in case of the light controller, all nodes of a group can fail. Therefore the protection requirement category for integrity has to be high.

As the physical location of the node is an optional item, the availability of this information is not important.

The protection requirement classification for configuration data is summarized in Table 3.

Table 3. Protection requirement classification: configuration data

Information	Confidentiality	Integrity	Availablity
Configuration data	normal	high	high
– Transport address of group	normal	high	normal
– Transport address of controller	normal	high	high
– Physical location of node	normal	high	normal

3.4 Cryptographic Keying Material

To determine the importance of the security objectives for the keying material it is necessary to understand the purpose of the keys, which is to enforce confidentiality and integrity for the system. Thus, the keys protect all information in the system. The confidentiality of the keys derives from the sum of all confidentiality and integrity classifications. If all data can be disclosed, the privacy of the occupants is endangered. This corresponds to the PRC high. The possibility of manipulating all data within the system might lead to financial losings because of heightened power consumption or to physical injuries. Finally, by breaking the confidentiality of the key, the keying material itself can be changed. Thus the protection requirement category of the key's integrity also has to be included. The resulting protection requirement category for the confidentiality of the keying material is therefore high (see Table 4). Manipulating the keys might result in communication problems. If one or more nodes believe the key to be different, they can no longer take part in the communication. Therefore the protection requirement category has to be derived from the overall availability category. Additionally, this might enable the attacker to infiltrate her own keys and thus break the confidentiality of the systems data. The protection requirement category is therefore high.

The loss of the keys has the same effect as either a confidentiality breach of the keying material, if the communication is continued without the protection of the keys or the unavailability of state information if no communication occurs without the keys. For both cases the PRC for the keying material is high.

Table 4. Protection requirement classification: encryption keys

Information	Confidentiality	Integrity	Availablity
Encryption keys	high	high	high

4 Discussion

Identifying the protection requirements of an information system is an essential part of each security analysis. It helps understanding the application domain, threats, and defining possible countermeasures. The application domains building control and home automation are well understood for wired networks that

use mesh-under routing, i. e., addressing and forwarding happens "under the hood" of IP (if IP is involved at all).

Security concerns are very low in this scenario as the network is isolated, hence rising the costs for an attack. As long as the invest in breaking into this network exceeds the potential gain, there is little incentive to do so. Even if the damage that a security breach might cause was high, the low probability of occurrence still can justify from an economic perspective not to use better security measures.

The risk is increased substantially when the network is not isolated any more: Wireless communication can facilitate intrusion where attackers manage to get into the coverage area of the radio signal. And even worse, interconnecting the building network with the global Internet opens the door for all sorts of remote attacks seen in the Internet today.

Well-known countermeasures exist and are in frequent use not only for secured company networks but also for today's low-budget networking devices at home. For feature-rich devices and broadband connections, the overhead introduced by strong cryptography is not a major concern. Notwithstanding the actual protection requirements, application designers can follow traditional security guidelines and select the most powerful security technology that is available.

For the Internet of Things, where devices can be very limited in their capabilities, this approach is not feasible any more (cf. [17]). Bergstrom et al. [18] propose an architecture that imposes a gateway that shields the home network from the public Internet. Access to the Web-based remote interface is protected by strong cryptography while the dedicated point-to-point link to the home appliance uses a more light-weight protocol for exclusive communication with the access gateway.

One disadvantage of this intermediary-based approach is that it abandons end-to-end security and potentially leads to a vendor lock-in and constricts the evolution of M2M-applications—the foundation of the Internet of Things.

Where end-to-end security is required and light-weight cryptography is inevitable because of the devices' limitations, it is crucial to identify the actual protection requirements to avoid unnecessary cost on one hand, and too weak protection of resources on the other.

In our paper, we have presented an analysis of protection requirements for light control in a typical home environment. Using the classification from [15] only the classes "normal" and "high" were used. Conditions that would call for "very high" protection are hardly imaginable. As a result, key length and initialization vectors might be shorter in this scenario compared to applications where danger for life and limb is expected. Although the same security functions are applied, these provisions mean less overhead in transmission and processing, and hence lead to less power consumption.

The main effects of security breaches we have identified are: Disclosure of personal information, altering the state of the light bulbs so that the lights can be switched off and forcing the light bulbs to keep their last state, which means

they do not react to pressing the switch. All of these consequences correlate to PRC high.

Our analysis shows that the impact of security breaches differs significantly for the distinct security objectives. Confidentiality breaches only have PRC high where state information is concerned, because these might reveal details about the habits of the occupants. Apart from that, only the encryption keys are confidential. This is not surprising as the secret keys are confidential by definition.

The integrity of the various data in the system is always PRC high. Every manipulation of data in the system might lead to the light bulbs to be switched off although they are supposed to be on. Therefore, it is essential to protect data integrity in the system.

In general, availability violations are less severe than integrity breaches. If the unavailability of data has consequences at all, these are almost always that the light bulbs keep their current state. Although this is correlated to PRC high, this does not pose a danger as severe as a sudden switch-off of the lights. In the former case, the occupant is used to the current conditions of his environment. In the latter, the environment of the user suddenly changes, which comes more unexpected and might startle the occupant. Therefore, the protection of data availability is important, but not as important as the protection of integrity.

In summary, integrity is the most important security objective in our scenario. Availability breaches are less severe, but might still have high impact. Confidentiality violations are only significant where state information is concerned. For other building control tasks such as HVAC, we anticipate similar results. That means, certain sensor values and configuration data have lower protection requirements than, e. g. control messages and the exchange of keying material.

This has consequences when selecting cipher suites for smart object communication: Where confidentiality is optional (e. g. for distribution of configuration data), cipher suites or modes that provide only data integrity could be used. For cipher suites that can provide both, data integrity and confidentiality, at the same time (such as Authenticated Encryption with Associated Data, AEAD, [19]), this knowledge is less important. Still, it helps selecting reasonable key and nonce lengths which is important to save bandwidth. memory and processing time.

5 Conclusions

In this paper we have demonstrated how protection requirements can be inferred for a given M2M communication scenario, with a specific interest on constrained devices.

Our paper gives a detailed overview of the damages security breaches might cause in a home automation scenario. This is the prerequisite for choosing the appropriate countermeasures to protect the data in the system. A subsequent risk assessment will help identifying where strong security is required. In constrained networks, devices are not able to manage security protocols with a considerable overhead, hence it is preferable to use light-weight security where this gives reasonable protection.

In the application scenario we have investigated, only normal and high protection is required. We argue that in general, these protection requirements classes allow for weaker cryptographic functions as if very high protection was necessary. Many applications in building control and home automation share this property.

When designing a secure system, the classification of protection requirements also helps selecting proper cryptographic functions that have as little overhead as possible. As an example, where confidentiality is less important than data integrity, the data may be only signed but not encrypted before transmission where this is more resource-conserving.

In summary, our approach helps designing effective security for constrained node networks. We anticipate that light-weight security mechanisms can be used safely in most M2M application scenarios, including resource management tasks and monitoring resource usage in the Internet of Things.

References

1. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey. Computer Networks 54(15), 2787–2805 (2010)
2. Mulligan, G.: The 6LoWPAN architecture. In: 4th Workshop on Embedded Networked Sensors (EmNets 2007), pp. 78–82. ACM, New York (2007)
3. Deering, S., Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (1998)
4. Pandey, S., Kim, M.-S., Choi, M.-J., Hong, J.W.: Towards management of machine to machine networks. In: 13th Network Operations and Management Symposium (APNOMS), pp. 1–7 (2011)
5. Bormann, C., Castellani, A.P., Shelby, Z.: CoAP: An Application Protocol for Billions of Tiny Internet Nodes. IEEE Internet Computing 16(2), 62–67 (2012)
6. Stallings, W.: SNMP and SNMPv2: the infrastructure for network management. IEEE Communications Magazine 36(3), 37–43 (1998)
7. Shelby, Z., Hartke, K., Bormann, C., Frank, B.: Constrained Application Protocol (CoAP). Internet-draft (2012), `http://tools.ietf.org/html/draft-ietf-core-coap` (work in progress)
8. Kovatsch, M., Weiss, M., Guinard, D.: Embedding Internet Technology for Home Automation. In: 15th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2010), Bilbao, Spain (2012)
9. Harrington, D., Schoenwaelder, J.: Transport Subsystem for the Simple Network Management Protocol (SNMP). RFC 5590 (2009)
10. Rescorla, E., Modadugu, N.: Datagram Transport Layer Security Version 1.2. RFC 6347 (2012)
11. Garcia-Morchon, O., Keoh, S., Hummen, R., Struik, R.: Security Considerations in the IP-based Internet of Things. `http://tools.ietf.org/html/draft-garcia-core-security`. Internet-Draft (2012) (work in progress)
12. Padmavathi, G., Shanmugapriya, D.: A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. International Journal of Computer Science and Information Security (IJCSIS) 4(1 & 2) (2009)
13. Arkko, J., Keranen, A.: CoAP Security Architecture. `http://tools.ietf.org/html/draft-arkko-core-security-arch`. Internet-Draft (2011) (work in progress)

14. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Communications of the ACM 47, 53–57 (2004)
15. Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2. Version 2.0. IT-Grundschutz Methodology (2008), https://www.bsi.bund.de/cae/servlet/contentblob/471430/publicationFile/28223/standard_100-2_e_pdf.pdf
16. Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30 (2012)
17. Potlapally, N.R., Ravi, S., Raghunathan, A., Jha, N.K.: Analyzing the energy consumption of security protocols. In: 2003 International Symposium on Low Power Electronics and Design (ISLPED 2003), Seoul, Korea, pp. 30–35 (2003)
18. Bergstrom, P., Driscoll, K., Kimball, J.: Making home automation communications secure. Computer 34(10), 50–56 (2001)
19. Rogaway, P.: Authenticated encryption with Associated-Data. In: Ninth ACM Conference on Computer and Communication Security (CCS-9), pp. 98–107 (2002)