Future Generation Computer Systems 56 (2016) 719–733

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A risk analysis of a smart home automation system

Andreas Jacobsson [a,*], Martin Boldt [b], Bengt Carlsson [b]

[a] Department of Computer Science, Malmö University, 205 05 Malmö, Sweden

[b] Department of Computer Science and Engineering, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden

HIGHLIGHTS

- Smart home automation systems introduce security and user privacy risks.
- A risk analysis of a smart home automation system is designed and conducted.
- 32 risks are identified, of which four are classified as severe and 19 as moderate.
- The severe risks are related to the software components, as well as human behavior.
- It is concluded that security and privacy should be integrated in the design phase.

ARTICLE INFO

Article history:
Received 13 November 2014
Received in revised form
11 June 2015
Accepted 4 September 2015
Available online 14 September 2015

Keywords:
Internet of Things
Smart home automation
Risk analys
Privacy
Security

ABSTRACT

Enforcing security in Internet of Things environments has been identified as one of the top barriers for realizing the vision of smart, energy-efficient homes and buildings. In this context, understanding the risks related to the use and potential misuse of information about homes, partners, and end-users, as well as, forming methods for integrating security-enhancing measures in the design is not straightforward and thus requires substantial investigation. A risk analysis applied on a smart home automation system developed in a research project involving leading industrial actors has been conducted. Out of 32 examined risks, 9 were classified as low and 4 as high, i.e., most of the identified risks were deemed as moderate. The risks classified as high were either related to the human factor or to the software components of the system. The results indicate that with the implementation of standard security features, new, as well as, current risks can be minimized to acceptable levels albeit that the most serious risks, i.e., those derived from the human factor, need more careful consideration, as they are inherently complex to handle. A discussion of the implications of the risk analysis results points to the need for a more general model of security and privacy included in the design phase of smart homes. With such a model of security and privacy in design in place, it will contribute to enforcing system security and enhancing user privacy in smart homes, and thus helping to further realize the potential in such IoT environments.

1. Introduction

In the near future, it is estimated that somewhat 90 million people around the world will live in smart homes, using technology to improve home security, comfort, and energy usage [1]. A recent study has shown that more than every fourth person in Sweden feels that they have poor knowledge and control over their energy use, and that four out of ten would like to be more aware and to have better control over their energy consumption [2]. A solution is to provide the householders with feedback on their energy consumption, for instance, through a smart home automation system [3]. Studies have shown that householders can reduce energy consumption with up to 20% when gaining such feedback [2,3]. Smart home automation is a prime example of a smart environment built on various types of cyber–physical systems generating volumes of diverse, heterogeneous, complex, and distributed data from a multitude of applications and sensors. Thereby, such home automation is also an example of an Internet of Things (IoT) scenario, where a communication network extends the present Internet by including everyday items and sensors, which in this case includes the possibility to monitor and manage energy usage [4]. As such, smart home automation systems incorporate common devices that control features of the home, but they do not only turn devices on and off [5]. For instance, smart home automation systems can monitor the configuration of the internal environment and the activities that are being undertaken whilst the house is

* Corresponding author. Tel.: +46 709 655 209; fax: +46 40 665 76 46.
E-mail address: andreas.jacobsson@mah.se (A. Jacobsson).

http://dx.doi.org/10.1016/j.future.2015.09.003
0167-739X/

occupied (and unoccupied). The result of these modifications to the technology is that a smart home automation system can autonomously operate devices and thus manage the home on behalf of the end-users, i.e., humans.

Smart home automation is attracting more and more attention from commercial actors, such as, energy suppliers, infrastructure providers, and third party software and hardware vendors [6,3]. Among the non-commercial stakeholders, there are various governmental institutions and municipalities, as well as, end-users. Knowledge, tools, and infrastructures related to software and data have begun to evolve in order to cover the challenges brought on by the complexity and the heterogeneity of massively interconnected services and devices, but there is at this point no well-established practice to design such intelligent systems [7]. For instance, accepted reference architecture alternatives or software platforms, let alone such that include otherwise crucial system requirements, such as, security and privacy in the process are currently missing [7,8]. As a result, there are multiple vertical solutions where vendors claim to support the whole chain from the sensors and devices to the gateways and servers, with whatever dedicated software that is appropriate in the perspective of the specific company. For example, this includes highly specialized APIs for the integration of additional services on top of the existing solutions. This creates a complex situation where, among many things, it is hard to avoid customer lock-in, something which may further smother their involvement and commitment. As a consequence, this also creates difficulties for executing system-hygienic tasks, such as, analyzing risks, enhancing privacy, and enforcing security in these environments.

In a joint research project involving leading industrial actors in the segment of home/building automation, a common interface of a smart home automation system (hereinafter denoted SHAS) that combines various vendors' systems has been developed.[1] Using SHAS, it is possible to transparently manage several smart home automation systems simultaneously in real-time. It is also possible for third party stakeholders, such as, property owners and municipalities, to both monitor energy consumption and remotely control electronic devices in the homes and buildings. Furthermore, end-users (e.g., as tenants) can collect aggregated energy consumption statistics on their buildings (e.g., from the owners). Based on the collected data, various services can be implemented, primarily as a way to raise the energy-awareness among end-users, e.g., by using gamification approaches. Also, on top of the common interface, an open mobile platform for energy efficiency services allows end-users to access various applications through an ecosystem of online services and smartphone applications. Through an open API, it is also possible for third party developers to connect their services and applications. In the research project, SHAS is tested on an apartment complex situated in Malmö, Sweden.

In IoT systems, particularly in those that involve human actors, such as, our SHAS, understanding the risks related to the use and potential misuse of information about customers, partners, and end-users, as well as, forming methods for integrating security-enhancing measures in the design is not straightforward and thus requires substantial analysis [4,9]. In addition, measures ensuring the IoT architecture's resilience to attacks, such as, authentication, access control, and user privacy need to be established [10]. In fact, the difficulty in achieving security in IoT environments has been identified as one of the top barriers of smart home automation [7], underlining that this is a cumbersome, yet important task.

In this paper, we apply a common risk analysis method in order to evaluate system vulnerabilities and threats, as well as, their likeliness of occurrence and potential impacts, i.e., the system's risk exposure. The analysis of risk exposure in SHAS is thus based on the well-known Information Security Risk Analysis (ISRA) method, documented by, e.g., Peltier [11]. The application of ISRA on SHAS is founded on a review of current advancements in science and industry. In order to fully understand the scope of the consequences brought on by smart homes, it is crucial to analyze not only the system risks related to privacy and security, but also the types of scenarios with respect to user privacy and home security that they entail. The main contribution is thus the results of the risk analysis on the smart home automation system in combination with the scenarios highlighting the consequences to user privacy and the review of the state of the art.

The paper is organized as follows. First, we set the scene by introducing the potential risk scenarios with respect to security and privacy of smart home automation. Then, related work, the architecture of SHAS, the ISRA method and its results are accounted for. This is followed by a discussion about the general risk exposure in relation to the main observations from the literature and scenario descriptions. In the end, conclusions and pointers for future work are summarized.

2. Scenarios of the private/public home

Before examining the risk exposure of SHAS by applying ISRA, we pinpoint some common scenarios for smart home automation systems. These scenarios have emerged as a result of discussions with key stakeholders within the smart home automation industry, i.e., the industry partners of the project management group of SHAS.

Property, as well as, users and the information that they are generating constitute an integral part of smart home automation, and as smart home automation systems become increasingly more adopted by residents, these system-infrastructures are also gaining more interest from other industry sectors. This is much due to that smart home automation systems introduce a valuable platform for direct user involvement, often through various connected sensors within the home environment where users and property interact through tablets, smartphones, computers, and various wearable devices. Future possibilities to extend the benefits and services of smart home automation will emerge that bring about a risk of concept drift. Basically, new vendors benefit from the context-aware smart home infrastructure, for instance, by exploiting the possibility of adding novel products and services to the ecosystem. Vendors take part in ecosystems, with business connections to various other vendors, rendering in that security and privacy concerns are often neglected or ignored. Another side of this is that the system (in our case SHAS) is reconfigured and equipped with new devices and software not included nor taken into account in the original design, rendering in that the system must be considered to be neither stable nor static; it is dynamic and changes all the time, and also in ways that are difficult to predict.

To shed some light on scenarios entailed by this development, we will now discuss the incorporation of safety surveillance cameras within a smart home, digital traces, and the addition of connected devices in smart homes. Below, these scenarios are briefly introduced and are then revisited in 7.

2.1. From energy efficiency to safety surveillance cameras

Even though smart home automation systems, such as SHAS, may be originally intended for energy efficiency support, it can be extended to include also other types of appliances in the homes. In smart homes, the use of a safety surveillance camera typically has a purpose to detect anomalies in the home environments, i.e., events that differ from the daily use. A first example of such an anomaly is

[1] More information can be found at http://elis.mah.se/ Last accessed: 2015-06-02.

using a surveillance camera to detect or verify fire from remote locations, e.g., rule out false alarms so that emergency services can be called. Such applications are already in use, but must be installed in safe-critical areas of the home, e.g., close to entrance doors and in bedrooms. Besides the obvious problem of automatically distinguishing a normal case from an abnormal, this kind of application also involves human interaction; someone needs to confirm what is happening. This may cause serious privacy concerns, i.e., someone may monitor everyday life in the home environment as the result of a (out of purpose) transmitting camera.

The surveillance camera can also be used for other personal purposes, such as, to see who is at home with respect to, e.g., childcare, control of infants sleeping, elderly care, etc. Home related performance statuses are also possible to monitor, e.g., if lamps are switched on or off, doors closed or open, cameras showing water leaks, etc. Smart home surveillance cameras can also be used in combination with other sorts of connected devices, which together may provide an overly detailed image of the persons living in that home.

Extending the use of smart home automation by including, for instance, surveillance cameras increases the risk of concept drift, i.e., when information is collected for one purpose, the same information can also be used for other intentions. Such extension of usage also typically raises the need for increased security restrictions, especially in terms of features enabling remote access to home cameras possibly involving persons in their private state. The main concern is whether comprehensive analyses of all possible threat scenarios are considered during such a continuous extension to the smart home automation infrastructures that are currently evolving in the industry, and to what extent autonomous decision-making by the system (and the vendors behind it) should be allowed.

2.2. Discovering digital traces

Besides linking together different equipment and system functions, as well as, including the data that these are handling, a potential intruder may acquire an undesirable level of knowledge about the residents of a home. As an example, measuring the overall power consumption provides a limited knowledge of the home, but the addition of individual measurements per electrical device (usage extent, time of day, etc.) generate more fine-grained meta-information about the family members' habits. To reduce energy consumption, detailed power measurements should ideally be produced. This motivates and facilitates, for instance, the use of user-oriented applications, usually available in the everyday life, e.g., through the use of smart phones, to be connected to the home. Combined, these applications, typically developed for other purposes, bear potential to evade user privacy and jeopardize home security in ways that can be difficult to anticipate.

Digital traces that the users (more or less voluntarily) leave behind when using the system can be used for building extensive personal profiles of the residents of a home. A burglar may remotely monitor routine activity patterns based on when persons in the household are at home, and thus get the means to conduct the burglary when the house is empty. It is also possible to create estimates about the activities that the household members are involved in based on unique appliance-specific electrical consumption break down [12]. For instance, novel methods allow the use of individual appliances to be filtered out from the overall consumption pattern with an accuracy of around 90%. This allows a smart home automation system to separately monitor the time and duration of use of, for example, dishwashers, various lights, kettles, TVs and video-game consoles [13]. Such monitoring activities can be seen as the equivalent of the mapping process, e.g., between users and their interests, that takes place on many parts of the web today, such as, Google-sites or Facebook, and may in the future be part of a larger mapping scheme where various (physical) user habits are plotted. The result may be a detailed personal dossier of information that contain not only a user's digital behavior, but also such that take place in the ordinary physical world. This, of course, means a bundle of highly sensitive information that, in the wrong hands, may be a severe threat to user privacy.

Since this type of information is delicate in the sense that there is a risk for misuse with severe consequences, such as, unsolicited commercial message exposure, stalking situations, etc. It must be clear to the end-users, what information out of all the information in flux in the smart home that is of a personal nature, how it is processed and distributed once it has entered the smart home automation system through an IoT device or sensor, and what part the user can play in this process. There is of course also a conflict between the service providers and consumers; the former want to collect as much information as possible for future reference or business opportunity, while consumers primarily only want to reveal small pieces of information that is useful at a certain point in time.

Therefore, it is important to investigate what actual choice the users face regarding their participation in the data collection process. In order for the users to be able to make an informed decision about adopting a smart home automation system, it is crucial that vendors of such systems are transparent about how personal data within the system is processed, analyzed, interconnected, and correlated. Without such transparency, it is hardly possible for users to provide the system with an informed consent, something that any user participation should be based on. A main concern therefore is the data in flux of smart homes; what does it look like, how can it be exploited by the connected devices (and in connection, the vendors behind them), and how should the support for enforcing user privacy be designed.

2.3. Augmenting the internet of things in smart homes

A popular application area in smart home automation is to use energy control as a means to avert burglary, for instance, by autonomously scheduling the lights to include also other types of electronic connections, such as, Internet-connected radio or TV at times when the home is unoccupied. This may also be done without the interaction of the user, i.e., connected objects in smart home automation systems can act autonomously based on, e.g., their capabilities to learn from the user's behavior. As more devices are involved in this scenario, an increased scope of data may be added to the system as a sort of random noise, thus making monitoring capabilities of smart home automation, as mentioned above, more difficult to deploy. This added feature is of course the opposite of ensuring energy efficiency in terms of the amount of power available only when needed. However, as the scheduling of electrical devices may convince potential burglars to avoid breaking entries, as well as, limiting the means for monitoring users in their homes, it may instead contribute to the enhancement of user privacy.

Moreover, by using energy control appliances in such a way, a drawback may be that the home can become physically vulnerable to new threats in the form of intrusion attempts that are usually associated with traditional online interaction, e.g., exposure to malicious software programs and through participating in online social networks. A security analysis must thus take into account the level of autonomy provided by the system (i.e., what decisions that can be made by the system without the involvement of a user), as well as, the general awareness of security and privacy with the user. This is an extension of security analysis to also include situations where no actual (human) user is around, but where the user unexpectedly may play an important part in the

resilience and security configuration (or lack thereof) of smart homes. Meanwhile, the connected smart home objects usually have limited means for security-enhancing measures, such as, encryption, and are also prone to environmental influences. As the objects can act without user awareness, they can control more than the digital side of the home, i.e., also the physical environment. A main concern therefore is the significant abuse potential brought on by this development of the smart home technologies, and an interesting question is how security should be designed to prevent intrusions and contribute to the concept of a private, yet connected home.

3. Related work

The reviewed related work presented below has been assimilated based on the research field of the project, i.e., smart home automation, and on the scenarios as introduced above. The account for related work is grouped in four sections, based on the main theme of the reviewed work, and in the end, some general observations are presented. The results of this study are also incorporated in the ISRA design, as described in 5.

3.1. Risk analysis-based approaches

The domain of smart home automation is viewed as a key element of the future Internet [5]. As homes are increasingly computerized and filled with devices ranging from smart TVs to home energy management systems, potential computer security attacks and their impact on residents need to be investigated. Denning et al. [6] survey the security and privacy landscape in IoT-based smart home environments, and provide a strategy for reasoning about security needs. They use a method based on three components that include the feasibility of conducting an attack, the attractiveness of the system as a compromised platform, and the damage caused by executing an attack. The first two factors, when combined, provide some indication of the likelihood that an adversary will compromise the device in question, while the third factor helps to weigh the overall risk. The goal of this is to facilitate an informed discussion about the potential risks with a technology if security is not sufficiently addressed in its design. As such, their framework provides a skeleton for characterizing risks, i.e., persons not accustomed to considering attack scenarios might require additional guidance. A strong merit with the paper by Denning et al. [6] is the framework for articulating key risks associated with particular devices in the home, which includes identifying human assets, security goals, and device features that may increase the risk posed by individual technologies, but since the devices and technologies used in the digital home are grouped together, the framework excludes technical nuances, such as, those entailed by problems with, e.g., transport encryption of data, limited CPU-storage on connected units, etc. Another merit is of course their approach to evaluating risk, but it is tuned for existing smart homes, rather than to support the development phase of smart home automation systems. However, they conclude that the new capabilities of home technologies enable novel attacks and at the same time allow some traditional attacks to have new consequences. There is thus a need for including a broad scope of risks, i.e., old, as well as, new ones, in smart home automation environments, something which is not further elaborated on in their work.

The belief that the introduction of smart home automation systems adds new risks in addition to existing ones is confirmed in the work of Roman et al. [14], where, e.g., an account for threats based on security and privacy perspectives is provided. This account is based on reasoning about system components in the connected home, i.e., the article does not address any empirical work. While they reason about various security threats and their mitigating countermeasures, they do not provide any information on how to identify the risks that are present and how they should be perceived. They conclude that, in order to manage the variety of threats facing IoT-connected homes, important problems to discuss are, e.g., data and identity management, user privacy, self-management, and methods to support resilient architectures.

Djemme et al. [15] have proposed a risk assessment framework and software toolkit for cloud service ecosystems, of which the digital home is viewed as an example. They stress that concerns, such as, risk, trust, security, cost, and legal factors underpin the non-functional properties of the ecosystem, and thus highlight the importance of effective risk management methods. The main contribution is the risk assessment model, which comprises four risk categories, in this case, legal, technical, policy, and general. As such, it excludes the otherwise important user perspective, which of course is central to any risk analysis of the smart home.

Kirkham et al. [16] explore cloud computing in the context of home resource management and propose a risk-based approach to wider data sharing between the home and its external services using key indicators related to risk, trust, cost, and efficiency. The risk model is based on a use case for home resource management and provides means to calculate the legal risk, the appliance failure risk, and the resource security risk. The legal risk calculus, which is a rule-based model, is innovative, as it addresses data sharing and legal compliance of the service provider in terms of privacy legislation and wider data processing law. Application to failure risk is concerned with elements of the environment that may cause the wider smart home applications to breach the legal agreement between householder and service provider. Resource security is concerned with possible threats to leakage of resources to both rogue service providers and malfunctioning devices. Although this apparently is an interesting approach, their empirical results are included only for two of the risk model categories, i.e., the legal risk calculus is left out. They point out the need for further study on the integration of risk calculation and the expression of risk in IoT-intense domains; especially in smart home environments inhabited by (human) users, where a lot of potentially sensitive data is in traffic. However, a general lack of quality data is acknowledged as a hindering factor in further developing the knowledge about risk exposure in IoT-connected homes.

3.2. Security-based approaches

In the work by Babar et al. [17], an embedded security framework for IoT environments is proposed. Based on a review of network-based attacks on IoT systems, they investigate the need to provide built-in security in the connected devices to provide a flexible infrastructure for dynamic prevention, detection, diagnosis, isolation, and countermeasures against successful security breaches. Based on this analysis, they define security needs while taking into account computational time, energy consumption, and memory requirements of the connected devices, i.e., while they set out to do a comprehensive view of security risks, they only focus on hardware and software components. They claim that security requirements for IoT will certainly underline the importance of properly formulated, implemented, and enforced security policies throughout their life cycle. However, in order to achieve this, risk analyses that fuel an understanding of both technical, as well as, human aspects, need to be applied to help define and motivate the security requirements of IoT-connected homes. Ning et al. [18] offer an IoT system architecture set to handle a broad array of challenges for enabling security, both at system, network, and application layer. Based on defining security in terms of requirements, such as, confidentiality, integrity, and availability, they conclude

that research efforts need to be put into advanced cryptographic protocols, data management solutions, and strategies to manage the tradeoff between security, privacy, and utility of IoT systems. They particularly highlight the importance of security-enhancing technologies in terms of cross-network authentication and authorization on the various cyberentities of, e.g., the connected home.

Gan et al. [19] focus on the application of technologies in IoT environments and target security-enhancing solutions to network points of entry. They say that major risks consist of instantiations of malicious software and various hacking techniques, and that they are important threats to mitigate by, e.g., authentication procedures in the connected devices and cryptography between the communicating objects. Although their work point to some relevant security issues, a conclusion from it is that much effort is still needed on further investigations on security design features in infrastructure and system planning, and that this requires a deep understanding of both impacting risk factors and of the technology itself. Their work is reflective, and they mostly reason about technical issues related to security, such as, encryption of gateway nodes, denial of service attacks, and authentication schemes. Van Kranenburg et al. [20] investigate security issues of communicating objects in smart home automation. They conclude that a significant research effort has been undertaken on cryptography tailored for low-cost, low throughput, and resource-constraint devices (referred to as "light-weight cryptography") in smart home environments. This particular circumstance, i.e., the resource-constrained nature of many of the devices in a smart home environment do not permit to implement the standard security solutions, which therefore make smart homes vulnerable to security attacks, is also supported by Lee et al. [21]. Van Kranenburg et al. [20] also explain that, in spite of the large number of available methods, there are few, which have been examined enough to be considered secure, and thus point to the need for methods that support the review of risk factors in smart home automation.

As pointed out by Das et al. [22], while mobile devices continue to grow in popularity and functionality; the demand for advanced ubiquitous mobile applications that support home security and surveillance also rises. Das et al. [22] have designed a home automation and security system (HASec) for mobile devices that leverages IoT technology to provide essential security-enhancing control functions. In particular, HASec operates and controls motion detectors and video cameras for remote sensing and surveillance, streams live video, records it for future playback, and manages operations on home appliances, such as, turning on/off a TV or microwave, or altering the intensity of lighting around the home. HASec has two main components interacting with each other; the iOS application that executes on the mobile device and the server-side scripts that run from a cloud server. Although HASec is a promising alternative for strengthening home security through smart home automation, the work by Das et al. [22] only addresses security measures, i.e., it does not include a risk analysis.

Notra et al. [23] dissect the behavior of household devices in connected homes, and highlight the ease within which security and privacy can be compromised. Based on this, they propose a solution to protect such devises, mainly by restricting access at the network level, i.e., the cloud service provider provides security as an overlay service not impacting the connected devices of the home. The most interesting part of their work is the experimental vulnerability analysis of popular smart home devices, in which they have pointed out the need for user-friendly and computer resource-efficient access-control mechanisms. The suggested security solution, i.e., access control rules in the home network, is thus a promising solution towards enforcing security and privacy in smart homes.

3.3. Privacy-based approaches

Arabo et al. [24] identify challenges and implications of privacy with respect to connected devices, of which some examples are identify theft, social engineering attacks, points of entry for a cyber attack, and social network-based threats, such as, grooming and cyber-bullying. This is an interesting discussion, but there is no evaluation of the severity of these privacy and security threats. They do, however, provide a discussion about the user data generated within the smart home, from which they draw the conclusion that malware management is a particularly important research challenge. Kozlov et al. [25] discuss threats to privacy and security at different levels of IoT architectures. With respect to the smart home, they especially advertise for privacy control mechanisms, methods to analyze privacy risk levels, and energy aspects of security, privacy, and trust, as they are closely related to energy consumption of the entire network infrastructure. Kozlov et al. [25] also highlight the need for legal support in the enforcement of privacy in IoT environments, and particularly stress the importance of taking privacy into account already while IoT systems are designed. Weber [10] explored privacy issues in the IoT with a special emphasis on judicial perspectives on technical components, such as, encryption, authentication, ID management, etc. He also studied users' rights, public awareness, disclosure statements, and user advocacy. From a legal perspective, Weber [10] analyzed user consent, collection limitation, use limitation, openness, and accountability, and proposed a legal framework on which a business is said to be able to rely on. He concluded that while according mechanisms still need to be developed, the early recognition of eventual problems and suggestions for their encounter need to be recognized before IoT environment, such as, a smart home, could be in full operation. While Weber's legal framework is conceptual, and does thus not include any empirical motivation, it is mainly focused on solutions to empower accountability rather than on the exposure of problems in terms of, e.g., privacy risks exposure. In spite of this, a legal platform, such as, the one suggested by Weber [10], is important in the development of IoT environments, as it is essential for businesses – and users – to be able to rely on a stable and foreseeable legal framework. Actually, this is an important aspect also of the security architecture of resilient smart home automation systems, which of course are dependent on stable and clear rules for business.

3.4. Industry-based approaches

There are a bundle of examples related to the ease, with which a smart home can be intruded, manipulated or hi-jacked. For instance, in a recent test of a smart home automation hub, security experts at Symantec found multiple security flaws that could allow attackers to gain access to the hub, as well as, to the devices connected to them [26]. For instance, if cyber criminals apply the, so called, ransom-ware model to smart homes, homeowners can find themselves coerced into paying a ransom in order to regain control of their heating, smart door lock, or smart TV. In smart homes, there are problems with complexity, competition between vendors, multiple incompatible standards resulting in inherent difficulties in achieving security and raising privacy, while also opening up for a scattered market situation. The resource-constrained nature of many of the devices present in a smart home environment does not permit to implement the standard security solutions and therefore smart homes are currently exposed to security vulnerabilities, of which the consequences are difficult to predict and evaluate [21]. Barnards–Wills et al. [27] point out that smart home service providers and technology developers may themselves become threat agents to other assets in the home. The key sources of such threats are often unintentional, i.e., they

Table 1
A concrete overview of the results from the study of related work presented in the order of appearance in 3. The ×-marks indicate the research focus of the work reviewed. On the last line, the ISRA approach as it was applied on SHAS is included. The ×-marks within parentheses indicate that even though the solutions to the identified privacy and security issues are not included per se in the empirical approach, these aspects are discussed in conjunction to the ISRA, i.e., in the three scenarios.

Research contribution	Research focus					Research method
	Risk analysis	Security issues	Privacy issues	Security solutions	Privacy solutions	
Denning et al. [6]	×	×				Scenario-based
Roman et al. [14]		×	×	×		Reflective
Djemme et al. [15]	×			×		Use-cases
Kirkham et al. [16]	×	×	×			Use-cases and data-based assessments
Babar et al. [17]		×		×		Scenario-based
Ning et al. [18]		×		×		Scenario-based
Gan et al. [19]		×		×		Reflective
Van Kranenburg et al. [20]		×	×	×	×	Use-case
Lee et al. [21]		×		×		Reflective
Das et al. [22]				×	×	System design
Notra et al. [23]		×	×	×	×	Experimental study
Arabo et al. [24]		×	×	×	×	Reflective
Kozlov et al. [25]		×	×			Scenario-based
Weber [10]			×	×	×	Reflective
ISRA approach applied on SHAS	×	×	×	(×)	(×)	Empirical evaluation and scenario-based study

relate to errors in design, installation, maintenance of devices and systems, as well as, the possibility of these providers being unable to fulfill their commitments due to, e.g., bankruptcy or stopping the support service for a previously installed product. These examples point to the need for risk analysis tools that can be adopted and used by end-users to enable informed decision-making on the configuration of smart homes.

Currently, there are countless initiatives occurring in the market for smart home technologies, as well as, in the media companies and in the organizations that cover it [27]. For instance, there are cloud computing security methods, such as, those provided by, e.g., IBM, and there are security protocols, such as, those provided by, e.g., Z-wave. In a white paper by Whitehouse [28], a guide for addressing considerations regarding cyber-security and privacy safeguards in IoT devices during its design and implementation is provided. According to the report it is crucial to manage any security considerations early on in the product development process by secure-by-default designs, i.e., that the default configuration settings are the most secure settings available. The National Technical Authority for Information Assurance in the UK publishes a list of 12 desired properties in secure-by-default platforms [29]. The first items on the list concern mandatory security controls for limiting access to both the CPU and memory capacity; although, quite obvious, the report states that such fundamental functions are hampered by legacy functionality on CPU architectures, such as, the x86 microprocessor.

While there are many industrial security providers for the smart home market in play at the moment, what seem to be missing are good practices and policy measures, such as, security standards. Good practices for the consumers include choosing systems that allow secure communication, local access, are not dependent on cloud services and use security features when they are available, which may well be deactivated by default. The standards relate to good practices in that they are certification approaches that seek to make the practices more widespread through the smart home industry. Even though standards are commonly viewed as a baseline requirement for manufacturers, the possibility of technology developing through standards and regulation should also be considered. In the report by Barnards–Wills et al. [27], an excellent overview of the current state of standards related to the smart home environment could be found.

3.5. Main observations

Based on the related work reviewed above, the following conclusions can be drawn:

- There is a general need for empirically based methods that support the evaluation of risks in smart home environments. Without such methods, the implemented security solutions risk not meeting the desired security and privacy goals of the smart home automation system.
- There is a general need for the integration of security in design. Risk analysis perspectives are typically put on the connected home from the outside, i.e., risk analysis is not included in the design and development phases of smart home automation systems and technologies. Security in design is crucial for mitigating the threats posed at IoT-connected homes, especially in terms of malware mitigation, access control, and privacy disclosure. Such sound security management must also contribute to the overall system requirements, something that is facilitated for during system development.
- The risks to user privacy need further specification. As information generated within the smart home often is of a personal nature, and thereby generally must be considered sensitive, exposure to privacy breaches needs attention to illustrate the potential breaches to the personal sphere of the home.
- The industry of security-enhancing mechanisms for smart homes is scattered pointing to the need for both good practices (for end-users) and policy measures in the shape of technology standards for system and service providers.

The risk analysis method used in this paper is selected based on its ability to address these needs, as is further explained in 5 (and especially in Table 1 of that chapter). Also, in 7, the main observations above will be discussed based on the results of the application of ISRA on SHAS. Before we go into that, the main architecture and functions of SHAS will be accounted for.

4. SHAS architecture

In smart home automation, energy services depend on a broad range of connected hardware and software components for monitoring and controlling an apartment or building [30–32]. In the case of SHAS, these sensors and actuators record and report

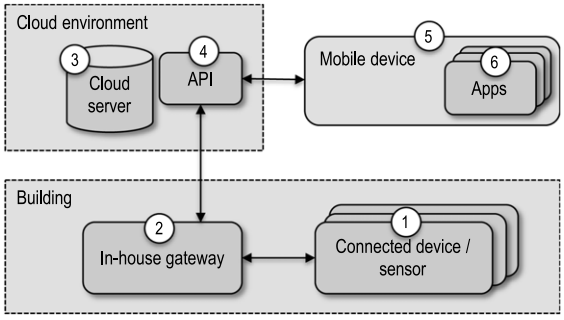

Fig. 1. An architectural view of the SHAS and the link to its physical devices. The numbers refer to the parts of the risk analysis described in 5.

metrics, such as, water usage, indoor temperature, CO_2 levels, and power consumption. Each device runs independently of each other and communicates using a local mesh network; in this case Zigbee (see, e.g., [33,34]) is used with a home gateway acting as the central node. The gateway runs a minimalistic Linux distribution and relays device information to a cloud server over the Internet using the XMPP protocol (see, e.g., [35]). In the SHAS architecture (as depicted in Fig. 1), it is important to effectively make use of the resources accessible higher up in the communication chain, as the availability of memory is limited on sensors and actuators. In an attempt to minimize the impact of outgoing Internet traffic, values are only reported from the in-house gateway if they deviate beyond a given threshold. Nevertheless, the gateway also has limited storage and computation capabilities, and in turn offloads data to the cloud server. Prior to this, the gateway also aggregates data over a certain period or within a certain interval.

The cloud server provides the platform with an API entry point that applications use to interact with the apartments in the building through the available devices. The platform API, however, does not grant access directly to the devices for application developers. Instead, the cloud server acknowledges an action to the application immediately and makes the necessary arrangements to ensure that a particular device's state is modified. For example, users wanting to turn off their bedroom lamps use their tablet computer to remotely perform this action. An API-call is then directed to the server over HTTPS, which immediately responds with a reference that the application can be used to verify that the desired state was entered. Alternatively, users may switch off the lamps manually. This state change must be propagated via the in-house gateway to the cloud server and, eventually, to applications and services in order to ensure that a consistent view of the device's state can be presented to the user. A representation of the device's state is thus stored at the server and this must be kept consistent by the actual device (as it is the true source).

The data provided through the API is a composition of several data sources, some provided manually by the user, some by external service providers, and obviously some by sensors on the actual device. The user, in turn, assigns contextual information to a connected device, such as, which appliance the smart devices control and where in the apartment they are located. This information is vital for application developers when, e.g., implementing smart shutdown of appliances based on user presence. From an application developer's perspective, the API exposes a composite set of information about devices and the basic services as part of the SHAS. Also, having externally contributed data, as part of the platform API, may unintentionally complicate error handling for the application developer. Furthermore, an API does not provide insight into which devices are available in an apartment only by describing the structure and exposed methods. Device types and their hierarchy must thus be communicated to application developers so that they do not misinterpret which aggregated data is already represented elsewhere.

The SHAS platform used for the connected devices is distributed across multiple hardware solutions manufactured by different companies, each with its own set of responsibilities and privileges. As the available devices in each apartment differ, each instance of the platform will subsequently be different. There are, however, some components that are fundamental for the platform's operational capacity, e.g., the in-house gateway for relaying messages that devices send over the local communication protocol (Zigbee or ZWave) to an Internet-based protocol (XMPP). Furthermore, there are devices that have strong temporal behavior, such as a user's mobile phone, which may be used as a contributor for determining the presence of a particular person, but cannot be guaranteed to always be present (or in itself always valid). In the analyzed prototype version of the SHAS, standard security features, such as, firewall on the cloud server and one-level authentication configuration in the mobile app, are included. However, in order to decide how security should ideally be configured, a risk analysis must be undertaken.

5. The information security risk analysis methodology

The reason for applying the ISRA approach in the development phase of SHAS is motivated based on the main observations made in the review of related work accounted for in 3. Proper and efficient integration of security in IoT-based smart home systems must be founded on the sound analysis of risk, i.e., the likeliness of loss [36,11]. In order to enable the identification of a reasonable level of security in SHAS, a methodology that embraces central security concepts like confidentiality, integrity, and availability, but also crucial processes, such as, prevention, detection, and response is thus useful. Successful IoT security strategies apparently also require a holistic approach, embracing all parts of the system while also contributing to fulfilling other system requirements. As is pointed out by Kirkham et al. [16], to be able to base the analysis of risk exposure directly on original quality data from within the system development is also an important characteristic for the credibility of the results. In addition to this, we wanted an analytical tool that enabled a deep understanding of the risks facing the system so that a discussion on the impact of privacy when making homes digital and smart can be possible. As can be seen in Table 1, there is also a general need for systematic, as well as, empirically founded way of analyzing the risk exposure of smart homes, something that is preferable to do before going into the implementation of security and privacy measures.

In the ISRA approach, the system's risk exposure is systematically reviewed based on its ability to fulfill the three basic goals of system security, i.e., confidentiality, integrity, and availability. The application of the ISRA approach has previously been applied, e.g., in the context of complex information exchange services in Internet-based collaborative networks (see, e.g. [37]) and in the context of analyzing the vulnerability of virulent computer programs in local area networks (see, e.g. [38]). The application of ISRA is based on empirical material gathered in the software development phase of SHAS, which will now be accounted for.

5.1. Practical approach

Decisions about risks should be perceived as choices under uncertainty, which, in our case, means that experts are consulted regarding the risk exposure of the SHAS architecture. The experts express their informed opinions in the form of probability distributions, which are aggregated into a single distribution that can be used for decision-making. In two collaborative workshop sessions including security experts, domain experts, and system developers of SHAS, in all nine persons, an open ISRA-questionnaire was used in order to reason, identify, analyze,

Table 2
Min, max, mean, and standard deviation for the probability, consequence and risk values calculated over all identified risks.

	Min	Max	Mean	Standard deviation
Probability values	1.0	4.75	2.27	0.86
Consequence values	2.0	4.0	3.23	0.46
Risk values	3.5	15.44	7.26	2.82

and evaluate threats, their linking to system vulnerabilities, as well as, their likeliness of occurrence and potential impact to the entire SHAS. During the workshop sessions each participant individually estimated the corresponding probability and impact associated with each threat based on a five level scale (1–5) ranking from unlikely/negligible to likely/disastrous respectively. Before the threat analysis started, the participants were briefed on how to interpret and use the different values on both probability scales to ensure a unanimous understanding among the participants, i.e., this took place prior to the identifications and estimations of the threats. After that, each identified threat received an estimated probability and impact value from each participant. The arithmetic mean of both the probability and consequence values was then calculated. Finally, a mean risk value, within the range (1–25) was calculated for each threat by multiplying the mean probability and consequence values.

In order to reduce complexity in the task, an information system-based approach to analyzing threats, vulnerabilities, and risk levels of the SHAS was applied. The architecture of SHAS was consequently viewed in analogy of an information system (see, e.g., [39]), and thus divided into subcategories containing software, hardware, information (or data), communication protocols (including radio communication), and the human actors (whether as end-users or as representatives for, e.g., vendors). This is an adaptation of ISRA, as this is not originally included in the design. However, it was deemed beneficial as it provides a measure to review both the system parts one by one and as a whole. The analyzed SHAS was divided into the following six parts (which are also mapped to the parts forming the architecture of SHAS, as illustrated in Fig. 1):

1. Connected sensors/devices (S).
2. In-house gateway (GW).
3. Cloud server (CS).
4. API (API).
5. Mobile device (MD).
6. Mobile device apps (App).

Each of the parts above was analyzed in search for vulnerabilities and threats related to hardware, software, information, communication, and human aspects in a structured way. If a risk was identified, it was given a unique descriptor (identifier) based on the system part and threat group it belonged to. For instance, the second software-related threat (S) concerning the in-house gateway (GW) is denoted S.GW.2, as can be seen in Table 4.

6. ISRA results

In this section, the results from ISRA applied on SHAS are presented. A total of 32 risks were identified during the risk analysis session. Each risk is represented by the following six attributes: a unique *identifier* according to description in the previous section, an explanation of the *vulnerability* exploited by the risk, an explanation of the *threat* that the risk poses, the mean *probability value*, the mean *consequence value*, and the resulting *risk value*. Both the probability and the consequence values are calculated using the input from the participants, both within the range (1–5), during the ISRA process. For each risk, a mean probability value and consequence value were calculated based on the estimates from each participant. The risk values were calculated by multiplying the mean probability and the consequence values, which produce a risk value in the range of 1–25. However, the lowest risk values measured within this study was 3.5 and the highest was 15.44. More information about the risk values and the mean probability and consequence values are available in Table 2.

On the average, consequences were classified as more severe compared to the probability of a certain risk that will happen. Also, there was a more expressed general agreement about the proposed consequences compared to the probability values. As a result, the combined risk values vary, resulting in that a subdivision is desirable. So, based on the risk values, each risk was classified into one of the following three severity classes: *low, medium, high*. The severity classes were defined as follows:

- Low: if risk value $<$ 6, i.e., the probability is unlikely to occur or the risk has a negligible impact.
- Medium: if risk value $\geq$ 6 and risk value $<$ 10.
- High: if risk value $\geq$ 10, i.e., both probability and impact are above a considerable value.

So, with respect to the five level scale, a low risk requires one of probability/impact factors to be low or if equal both should be below approximately 2.5. A medium risk includes the two highest values for one of the probability/impact factors only if the other factor is below approximately 3.0. A high risk requires that both factors be above approximately 3. Out of the total 32 risks, 9 were classified as low, 19 as medium, and 4 as high with respect to severity. In Table 3, the severity classification is shown for each risk divided into the six subsystem categories, as well as, the five threat categories. The threat category that includes most risks is the software-related category, which includes 13 risks. The threat categories concerning information, communication, and human all contain 5 risks each, while hardware-related threats contain 4 risks. Most highly severe risks are found in the human category.

Since the risk analysis was carried out close to the first system version delivery, i.e., after the integration of standard security-enhancing processes, the number of highly severe risks is rather sparse.

6.1. Identified risks

The identified risks from the application of ISRA on SHAS are presented in two steps. First, all risks are presented in five tables, one for each of the subsystem categories: *software, hardware, information, communication, and human*-related risks. Then, in step two, a more detailed analysis of the risks classified with a severity of either medium or high is carried out.

6.1.1. The software category

In Table 4, the software-related risks that were identified can be found. There were in total 13 software-related risks divided among the subsystem components as follows: 4 risks concerning the API, 4 concerning apps, 3 concerning the in-house gateway, and one risk each concerning the cloud server and mobile devices. The most probable risk relates to inadequate accountability within the in-house gateway, i.e., system events are not logged, which make them harder to trace at a later time. The most severe consequence is associated with inadequate authentication in the API. The highest risk value concerns unauthorized modifications of system functions in mobile apps, i.e., end-users can gain access to system resources without having proper credentials. The five software-related risks with the highest risk value are addressed in more detail in 6.2.

Table 3
A classification of risk severity as either Low/Medium/High based on the corresponding risk value. The risks are divided into five columns, one for each threat category, and six rows, one for each subsystem category.

Id	Software	Hardware	Information	Communication	Human
Sensors/devices	0/0/0	0/1/0	1/0/0	1/0/0	N/A
Gateway	0/3/0	0/1/0	0/2/0	0/1/0	N/A
Cloud server	0/1/0	1/0/0	1/0/0	0/1/0	N/A
Mobile devices	1/0/0	1/0/0	1/0/0	1/0/0	N/A
Apps	0/3/1	0/0/0	0/0/0	0/0/0	N/A
API	0/4/0	0/0/0	0/0/0	1/0/0	N/A
Total	1/11/1	2/2/0	3/2/0	3/2/0	0/2/3

Table 4
Identified threats with regard to software components within SHAS. Identified risks targeting sensors (S), the cloud server (CS), the in-house gateway (GW), mobile devices (MD), the API (API), and smart phone apps (App). The risk value indicates degree of exposure; the higher the value, the higher the risk. The standard deviation (std dev) of the probability and consequence values are presented within parentheses.

Id	Vulnerability description	Threat description	Mean probability value (std dev)	Mean consequence value (std dev)	Mean risk value
S.GW.1	Inadequate authentication (HTTP, SSL)	Unauthorized access to system	2.75 (0.50)	3.00 (0.82)	8.25
S.GW.2	Inadequate accountability	Unregistered system events	3.50 (0.58)	2.75 (0.96)	9.63
S.GW.3	N/A	Denial of service attacks	2.25 (0.50)	3.00 (1.41)	6.75
S.App.1	Inadequate authentication (HTTP, SSL)	Unauthorized access to system	1.75 (0.96)	3.50 (0.58)	6.13
S.App.2	Inadequate access control	Unauthorized modification of functions	2.25 (1.26)	3.25 (0.96)	7.31
S.App.3	Inadequate accountability	Unregistered system events	2.50 (0.58)	2.00 (0.82)	5.00
S.App.4	Software security in app	Unauthorized modification of functions	3.00 (0.82)	3.50 (0.58)	10.50
S.API.1	Inadequate authentication (HTTP, SSL)	Unauthorized access to system	1.75 (0.50)	4.00 (0.00)	7.00
S.API.2	Inadequate access control	Unauthorized modification of functions	2.25 (0.50)	3.25 (0.96)	7.31
S.API.3	Inadequate accountability	Unregistered system events	2.75 (0.96)	2.50 (0.58)	6.88
S.API.4	Software vulnerability in API	Unauthorized modification of functions	2.50 (1.29)	3.75 (0.50)	9.38
S.CS.1	Software vulnerability in MS Azure	Unauthorized modification of functions	1.50 (0.58)	3.75 (0.96)	5.63
S.MD.1	Software vulnerability in mobile device, e.g., OS	System manipulation and data leakage	1.25 (0.50)	3.25 (0.50)	4.06

Table 5
Identified threats with regard to hardware components within the system. Identified risks targeting sensors (S), the cloud server (CS), the in-house gateway (GW), mobile devices (MD), the API (API), and smart phone apps (App). The risk value indicates degree of exposure; the higher the value, the higher the risk. The standard deviation (std dev) of the probability and consequence values are presented within parentheses.

Id	Vulnerability description	Threat description	Mean probability value (std dev)	Mean consequence value (std dev)	Mean risk value
H.GW.1	Inadequate physical security	Theft, sabotage/destruction, and manipulation	1.75 (0.50)	3.75 (0.50)	6.56
H.MD.1	Inadequate physical security	Theft, sabotage/destruction, and manipulation	1.75 (0.50)	2.75 (0.50)	4.81
H.CS.1	Inadequate physical security	Manipulation, and possibly theft	1.25 (0.50)	3.75 (0.50)	4.69
H.S.1	Inadequate physical security	Theft, sabotage/destruction, and manipulation	2.00 (1.15)	3.25 (0.58)	6.50

6.1.2. The hardware category

In Table 5, the identified hardware-related risks are presented. There were in total 4 hardware-related risks divided among the subsystem components as follows: one risk concerning the in-house gateway, one concerning mobile devices, one concerning the cloud server and one concerning the sensors. The most probable risk relates to unauthorized modification/tampering of physical sensors, i.e., various manipulation scenarios on IoT sensors. The most severe consequence is associated with unauthorized modification/tampering of physical sensors or in-house gateway. The highest risk values concern unauthorized modification/tampering of in-house gateway, e.g., resetting the system in order to recover the default password.

6.1.3. The information category

In Table 6, the identified information-related risks can be found. There were in total 5 information-related risks divided among the subsystem components as follows: two risks concerning the in-house gateway, one concerning the cloud server, one concerning mobile devices, and one concerning the sensors. The most probable risk relates to inadequate access-control and authentication within in-house gateway, e.g., inadequate separation of privileges between user accounts. The most severe consequence is associated with the same risk concerning the in-house gateway, and as a result the highest risk value also belongs to that risk. This risk is also analyzed in more detail in 6.2.

6.1.4. The communication category

Table 7 contains the communication-related risks that were identified during the risk analysis. There were in total 5 information-related risks divided among the subsystem components as follows: one risk each among the sensors, cloud server, in-house gateway, mobile devices, and the API. The most probable risk relates to manipulation, duplication, surveillance, and deletion within sensors and the cloud server. The most severe consequence

Table 6
Identified threats with regard to the information/data processed within the system. Identified risks targeting sensors (S), the cloud server (CS), the in-house gateway (GW), mobile devices (MD), the API (API), and smart phone apps (App). The risk value indicates degree of exposure; the higher the value, the higher the risk. The standard deviation (std dev) of the probability and consequence values are presented within parentheses.

Id	Vulnerability description	Threat description	Mean probability value (std dev)	Mean consequence value (std dev)	Mean risk value
I.CS.1	Inadequate authentication and access control	Manipulation, duplication, surveillance, and deletion	1.50 (1.00)	2.50 (1.00)	3.75
I.GW.1	Inadequate authentication and access control	Manipulation, duplication, surveillance, and deletion	2.50 (0.58)	3.25 (0.50)	8.13
I.GW.2	Absence of, or inadequate access control policy and configuration	Inadequate authentication and access control	2.75 (0.50)	3.50 (0.58)	9.63
I.MD.1	Inadequate separation between different apps on device	Manipulation, duplication, surveillance, and deletion	1.25 (0.50)	3.00 (1.15)	3.75
I.S.1	Vulnerable comm. protocol	Data leakage and manipulation	1.50 (0.58)	3.00 (1.15)	4.50

Table 7
Identified threats with regard to communication channels utilized in the system. Identified risks targeting sensors (S), the cloud server (CS), the in-house gateway (GW), mobile devices (MD), the API (API), and smart phone apps (App). The risk value indicates degree of exposure; the higher the value, the higher the risk. The standard deviation (std dev) of the probability and consequence values are presented within parentheses.

Id	Vulnerability description	Threat description	Mean probability value (std dev)	Mean consequence value (std dev)	Mean risk value
N.S.1	Inadequate authentication and confidentiality	Manipulation, duplication, surveillance, and deletion	2.25 (0.50)	3.75 (0.50)	8.44
N.CS.1	Inadequate authentication and confidentiality	Manipulation, duplication, surveillance, and deletion	2.25 (0.50)	3.75 (0.50)	8.44
N.GW.1	Inadequate authentication and confidentiality over HTTP	Manipulation, duplication, surveillance, and deletion	2.00 (0.82)	2.75 (0.96)	5.50
N.MD.1	Inadequate authentication and confidentiality over HTTP	Manipulation, duplication, surveillance, and deletion	1.75 (0.50)	2.75 (0.50)	4.81
N.API.1	Vulnerability in network protocol used to access API	Manipulation and data leakage	1.00 (0.00)	3.50 (0.58)	3.50

is associated with the previous mentioned risks, and as a result these risks also got the highest risk values. This risk is also analyzed in more detail in 6.2.

6.1.5. The human category

Table 8 contains the identified human-related risks. In total, 5 human-related risks were identified, and obviously none of them are related to any system components since they concern situations related to human behavior. The most probable risk relates to poor password selection, which could lead to that authentication mechanisms are omitted. The most severe consequence is associated with two risks, the first concerns unauthorized redistribution of confidential information among system or cloud providers, the second concerns hacking exploitation attacks from various actors. The highest risk value altogether belongs to poor password selection. The risks of poor password collection and those relating to sloppy and gullible end-users are addressed in more depth in 6.2.

6.2. An analysis of the medium and highly severe risks and their corresponding mitigating measures

Below, we go through the risks with the highest risk values in each SHAS category, starting with the hardware-related risks. The hardware-related risks mainly concern theft, manipulation, and sabotage of the various devices and servers used within the SHAS. To mitigate these threats, we can conclude that appropriate physical and perimeter security is needed. Physical protection consists of one or more of these elements; deter, detect, alarm, delay, and respond [40]. This setup ranges from certified locks on door to guards responding on raised alarms.

Regarding the software risks, S.App.3 concerns software vulnerabilities in the mobile app of SHAS. Software vulnerabilities are ubiquitous in almost any computer system. They therefore convey the risk of attackers that could exploit these software vulnerabilities, using, for instance, buffer overflows or race condition vulnerabilities in the software. Information about known vulnerabilities, together with information on how to patch the vulnerabilities, is disclosed in a number of publicly available CVE (Common Vulnerability and Exposure) databases, e.g., CVE Details.[2] By making use of the information, software developers and security engineers can both contribute to a situational awareness, as well as, to pointing out useful mitigation and patching techniques. Also, in order to mitigate such risks, it is important to adopt secure coding practices and rigorous testing techniques, including penetration testing. Furthermore, it might be fruitful to deploy the use of signing the software based on cryptographic certificates and trusted third parties. In the risk S.API.4, the possibility of software vulnerabilities in the API, which could allow attackers to execute unauthorized actions through the API, is highlighted. Although a rather moderate risk value, this can allow for reading and/or modification of information in SHAS, which, if not attended to, can render the system vulnerable to information collection from multiple sources outside SHAS.

The software risk denoted S.GW.1 entails that the authentication mechanism is vulnerable to attack, allowing attackers to circumvent, e.g., password authentication schemes and thereby gain access to the system without proper credentials. To mitigate this risk, the use of standardized components for handling authentication and session control should be utilized over such components implemented within SHAS. Available methods for authentication range from traditional passwords, through public key infrastructure-based authentication to multi-factor authentication, which, for instance, include the end-user's cellphone. As always, it is important to continuously install software patches released for any software packages used to mitigate these types of risks.

[2] CVE Details can be found at http://www.cvedetails.com Last accessed: 2015-06-02.

Table 8
Identified threats with regard to human actors within the system. Identified risks targeting sensors (S), the cloud server (CS), the in-house gateway (GW), mobile devices (MD), the API (API), and smart phone apps (App). The risk value indicates degree of exposure; the higher the value, the higher the risk. The standard deviation (std dev) of the probability and consequence values are presented within parentheses.

Id	Vulnerability description	Threat description	Mean probability value (std dev)	Mean consequence value (std dev)	Mean risk value
U.1	Disgruntled employee, e.g., at third party contractor	Unauthorized redistribution of confidential information	1.75 (0.50)	3.50 (0.58)	6.13
U.2	Sloppy end-users etc.	Social engineering	4.25 (0.50)	3.25 (0.50)	13.81
U.3	Gullible users, etc.	Privacy threats, e.g., through gamification	3.50 (1.00)	3.00 (0.82)	10.50
U.4	Poor password selection	Circumvention of authentication mechanisms	4.75 (0.50)	3.25 (1.26)	15.44
U.5	System configuration	Hacking exploration attacks	2.75 (0.96)	3.50 (0.58)	9.63

Another software-based risk targeting the in-house gateway is S.GW.2, which represents inadequate accountability and logging settings. If realized, this may render in that system events remain unregistered in the system log. This can create severe problems in handling bug fixing, as well as, intrusion attempts, since changes and compromises to the system can become untraceable in the logs. Although this is currently handled in SHAS, synchronization of logging and registry activities need careful configuration and policy alignment, which of course need to be respected by all included parties. Although, as vendors of smart homes often have business relations with other vendors and thus take part complex ecosystem structure, this is easier said than done.

As is shown in the software risk S.GW.3, SHAS, like all systems, can be exposed to denial of service attacks due to its inherent property of publishing services, i.e., there is no explicit vulnerability connected to this threat. In SHAS, the configuration of the cloud server can enable flooding of messages to the in-house gateway, rendering in that the system becomes unavailable. This risk can, albeit ubiquitous in any computer system, be mitigated either by deploying in-house equipment from external vendors, or by benefiting from security techniques provided by Internet service providers, such as, traffic scrubbing filters and efficient client-puzzle approaches [41,42].

The highest ranked risk related to the information/data processed within SHAS is I.GW.2, which represents inadequate access control configuration in the in-house gateway. In the current version of SHAS, there is no access control mechanisms implemented since the in-house gateway only can handle a single user account, i.e., the administration user. However, for the future, where multiple user accounts on the in-house gateway will be mandatory, access control settings need to be in place. Another important task, also pointed out in [7], is to allow for temporary access to guest applications, devices, etc.

Within the category of network communication, the highest ranked risks concern inadequate authentication and confidentiality settings within the various connected sensors, as well as, in the remote cloud server. The risk labeled N.S.1 highlights the problem with sensitive information that can be transmitted between the sensors and the in-house gateway, e.g., commands with instructions to switch on/off electronic devices, such as, alarms and surveillance cameras. To mitigate this risk, such information should not typically be sent in clear text, and thus a secure (encrypted) communication protocol is needed in SHAS. In addition to protect against confidentiality threats, the protocol also needs to be able to resist manipulation threats so that the preconditions for replay attacks are minimized, i.e., that communication is recorded and later resent in order to carry out a task, such as, switching on a light. Although it is trivial to protect against replay attacks in traditional computer systems, the limited computing and power resources of typical IoT-connected devices bring about new challenges for this.

Furthermore, N.CS.1 highlights the risk concerning inadequate authentication and confidentiality configuration in the network communication between the various subsystems. This problem could be addressed using encryption and authentication schemes, such as, Transport Layer Security or Virtual Private Networks, that are regulated using legal contracts with the cloud service providers, as this relates to potentially sensitive user data transmission.

In terms of security, human actors represent a weak link in all computer-based information systems. As such, humans constitute a complex challenge to handle in any risk analysis of computer systems, which has proven to be the case also in SHAS. The highest ranked risk concerning human aspects is the deployment of weak passwords (U.4), which could be mitigated through the enforcement of password policies and verification tools. This is especially important in the single user account used within the in-house gateway. Furthermore, user accounts are often – when default configured – a weak point for hacking attempts and man-in-the-middle attacks. It is also important to recognize that the origin of the human-oriented risks span from gullible end-users that usually constitute targets in, e.g., social engineering attacks (U.3) to disgruntled employees that can either sell or deliberately leak confidential information in order to, e.g., make a profit or cause harm or inconvenience to the employer (U.2). The tools available for addressing these threats are usually grouped in policies and legal contracts, as well as, in education efforts of the end-users.

In the development of SHAS, software testing in order to identify bugs and other vulnerabilities has been deployed throughout the process, which, to some extent, is also the case with security analysis. This circumstance may explain the relatively low number of high risk levels identified in 6. Mainly, the most severe risks concern human actors, where mitigating measures rely more on how to inform or train users than to improve the technical design of the SHAS. Also, experience shows that system security needs constant attention in order to prevent, detect, and react to malicious or selfish intrusion or manipulation attempts. Nevertheless, the risk analysis has pointed out some serious flaws in the current system architecture. This is mainly handled by proposing improvements based on experience from related areas, i.e., using similar techniques with a similar scope. It is likely to believe that application areas with longer and more profound experience are more mature when it comes to security issues, and thus beneficial to learn from. We believe that the system must be designed to address deficiencies in a dynamic way by avoiding cumbersome built-in static security controls, e.g., by supporting programmable and thus adjustable solutions.

7. Discussion

As pointed out in 2, extending products and services to the residents of a smart home make it possible to collect additional information about the household. In the case of smart home automation, this process takes place in people's ordinary lives and typically without their understanding of the implications that this

collection may have on their privacy and home security. The digital traces that the users leave behind and that the various stakeholders can collect may also be combined and extended with more general personal data, such as, aggregated neighborhood statistics, to a personal profile making both home and user vulnerable to various intrusions. The use and misuse of information may thus affect the potential benefits of introducing smart home automation systems.

7.1. The need for risk analysis

As was concluded in 3, a general need for systematic and empirically based methods supporting the evaluation of risks could be observed in the literature, as well as, in the industry of smart home automation. This is something that has motivated the choice of empirical method in this paper, i.e., the ISRA approach. The application of ISRA has enabled a systematic review of the risks, i.e., as probable dangers, directed to a smart home automation system, in our case SHAS. The approach, when applied on SHAS, included both security experts and system developers in the risk analysis process, i.e., they provided access to original quality data. The particular choice of ISRA, with its semi-qualitative nature, was motivated in that risk analysis methods that use purely quantitative measures may not be entirely suitable in connected IoT infrastructures [29], such as, smart home automation systems, where systems have both a heterogeneous structure, complex relationships of connected devices and deployed software. Moreover, the ISRA approach is widely used in the security community [11]. When applying ISRA, there is often a need for the human mind to sift through the amounts of data and connections between them in order to identify and value the probable attack points. This particular circumstance might lead to that important conclusions about generalized probabilities and consequences are missed and that inconsistent results may be yielded. This also means that the results of the ISRA approach can be said to be depending on the experience of the people who conducted the risk analysis, which, however; also may be viewed as a merit (see, e.g. [11]). Even though, the application of ISRA on SHAS may not completely bridge the identified gap of general, systematic, and empirically based risk analysis methods in smart home automation systems, it can certainly be seen as a contribution to the general development in the area. So, we investigate the propagation of risks between different threat categories and different subsystems as seen in Table 3. Note that the actual risk values are used for separating risks into three severity classes (low, medium, and high), but no statistical comparison between single risks is done.

7.2. The need for security

It has also been concluded in 3 that there is a general need for security in design of smart homes, something which is also emphasized in [27,7]. As risk analysis perspectives are typically put on the connected home after the system is in place, i.e., risk analyses are usually not included in the design and development phases of smart home automation services and technologies, the application of ISRA aimed at contributing to bridge this gap. In the review of the risks facing SHAS, this was enabled through the inclusion of the security experts in the ISRA workshops described in 5.1. Security in design is crucial for preventing, as well as, moderating the threats posed at IoT-connected homes, especially in terms of malware mitigation, access control, and disclosure of personal information. Since the smart home systems may also be connected to other home devices, each with its own purpose, the original view of the security requirements (if any) may as a consequence be set aside. In addition, security perspectives on the development of IoT products for the connected home must also include indirect characteristics, such as, connectability, interoperability, and pervasiveness. It must also be taken into account that the smart home system typically belongs to an ecosystem of vendors, users, systems, etc., and that the potential cyber attacks surfaces thus increase in number while they at the same time become increasingly physical. Especially this last circumstance is important in smart homes, as it must be considered that privacy-sensitive devices, such as, surveillance cameras and personal wearables are likely to become parts of the smart home ecosystem. Another important aspect of the smart home that ideally should be dealt with in the development phase is data management. In smart home systems, a lot of data is in flux. As this data typically is generated by the user, or on behalf of the user, a large extent of it must be assumed to be personal, thus sensitive. With the dynamicity of smart homes, i.e., the configuration of system-connected devices changes over time in ways that may be difficult to predict, it is crucial that this aspect is taken into account at an early stage of the system development.

Even though all of the above mentioned aspects are difficult to include in the design phase, the ambition with the inclusion of security experts and system developers in the application of ISRA on SHAS was to highlight the role of security in system development. This means that there have been no methodological boundaries in including such aspects in the analysis and in the design. However, the relative openness of the ISRA approach of course also points to the need of a more systematic and purpose-oriented approach to fully integrate security in the design of smart homes.

7.3. The need for user privacy

A highly relevant area to explore in smart homes is the risks to user privacy. While more and more parts (and devices) of the home are connected to the Internet, users, as well as, various stakeholders can get access points to the whole system (i.e., the home), and not just to separate devices. This means that not only physical devices may be connected, but also that these devices, and the various stakeholders behind them, may get access to the smart home information in flux. A major challenge then is to find effective ways to provide users with a comprehensive picture of the entire system, and an indication of the sensitivity of data in transit, while also supporting the management of the home. Digital traces that the users (more or less voluntarily) leave behind when using a smart home system can provide meta-information about the family members' habits, i.e., help to build extensive individual and collective profiles of the residents of a home. In addition to the physical consequences that may occur as a result of this, e.g., in terms of burglaries, the idea of the home as a private sphere may no longer be accurate. Instead, the home may become a public area where the companies behind the connected devices will come to know a particular resident better than his/her closest friends or family do.

These types of perspectives are of course difficult to include in a systematic risk analysis approach, nevertheless they are important to identify and to reason about. To exemplify this, we accounted for scenarios of the private/public home in 2, in which we can conclude that albeit seeming distant it is important to include the use of surveillance cameras with the risk of concept drift, linkability between added system functions and data, as well as, the augmented use of various connected devices, of which some are user-intense. Even though these additions were not included as points of analysis in the application of ISRA on SHAS, they are highly useful in understanding the implications of the results of the ISRA approach. Based on this, we can conclude that the sound management of information generated within the system, i.e., without compromising either the system security or

the personal privacy of the user, is consequently a major challenge. The sensitivity, but also the risks and risk factors, related to how personal information is handled in the home environment and the ecosystem of people, machines, information, and actors that are included would consequently be interesting to explore further. In this analysis, the addition of social behavior of human actors (both as benevolent users and as villains) is a crucial characteristic. Strategies for the management of user-generated information in smart homes are another interesting area to explore. Also, methods for reducing sensitivity in information, such as, adjustable anonymity and linkability, as well as, data minimization and control should also be included in such an analysis.

Increasingly, the home is no longer a private closed environment. An important question in this respect concerns where to draw the line between public (or corporate) and personal information, e.g., as highlighted in the scenario of how to manage a surveillance camera. Instead of a static boundary, it would be beneficial if users (e.g., as tenants) themselves could in an easy and transparent manner configure the system according to their own privacy preferences. Good practices that can guide the end-users in this process are a promising approach. How information is collected, stored, and handled, as well as, what laws, policies, and standards that regulate this is another relevant issue, connected to the scenario of linkage between system functions and data. On this theme, it is of course important to ensure legal compliance given the obvious aspect of (accidental or intentional) privacy breaches as our scenario of misuse of user-intense devices suggests. Technical mechanisms regulating access to the collected information and how such access can be requested are also of great concern. Clear contracts of data sharing and usage are needed in the form of user data management services, proper service level agreements with third party actors, and methods for raising awareness of the possibilities, but also of the risks connected to smart home automation systems.

7.4. Security and privacy in design

The application and results of ISRA when applied on SHAS, the privacy risk scenario discussion, and the findings from the study of related work point to the need for the integration of security in the design phase of smart home system development, i.e., a model for security and privacy in design. The question then is how such a model should be designed, i.e., what the central components, etc., should be. Based on our research, we suggest that, at least, the following steps should be included in the model:

1. Identification and categorization of the personal data in transit in smart homes.
2. Analysis and description of the main risks to privacy and security.
3. Identification and implementation of preventive, detective, and reactive mitigating measures to reduce risks.
4. Strategy for privacy-friendly information management within smart homes.

The inclusion of developers and security experts in the application of ISRA has shown that this approach may be useful for the steps 2 and 3 in the development process of a smart home automation system. However, more work is needed to define a method for classifying the personal data that is generated, stored, changed, and distributed in connection to the smart home. This is also the case with the design of a strategy for the management of user-generated information in smart homes, as well as, in their connection to the digital ecosystems that they engage with. In addition, various methods for reducing sensitivity in information, such as, anonymization, data minimization and control are important to include in this analysis. An interesting idea is also to integrate security and privacy in the, at least partially, autonomous decision-making process of the connected entities that form the smart home system, as autonomy is already a prominent feature of various IoT solutions for the connected home. If such a model of security and privacy in design should be implemented, it would surely contribute to enforcing system security and enhancing user privacy in smart homes, and thus helping to further realize the potential in such IoT environments.

8. Conclusion

In a joint research project involving leading industrial actors in the segment of home/building automation, a common interface of a smart home automation system that combines various vendors' systems has been developed. Using this common interface, third party stakeholders can both monitor energy consumption and remotely control electronic devices in the homes and buildings. Open system architecture allows end-users to access various applications through an ecosystem of online services and smartphone applications. In this highly connected and complex environment, a systematic and empirically founded risk analysis method, which is widely used in the security community, and that is set to identify the most severe potential dangers has been undertaken.

In the application of the risk analysis, the architecture of SHAS was divided into five parts, i.e., software, hardware, information, communication protocols, and human actors. Out of 32 examined risks, 9 were classified as low and 4 as high, i.e., leaving that most of the identified risks were considered moderate. The risks classified as high were either related to the human factor or to software components. Furthermore, it was concluded that one of the main sources of risk is connected to the software, and especially in the APIs and within the mobile apps. The hardware-related risks concern theft, manipulation, and sabotage of the various devices and servers used within SHAS. The highest ranked risk related to the information processed within SHAS is derived from inadequate access control configuration in the in-house gateway. Within network communication, the main risks come from inadequate authentication and confidentiality settings. The most severe risk agent confirmed in the risk analysis is the human factor, i.e., as such; humans represent the highest risk exposure in smart home automation systems.

In the risk scenarios of smart homes, it has been shown that connected devices may cause undesirable consequences to user privacy with respect to, e.g., access to potentially sensitive meta-information, and the misuse of user-intense mobile devices, and the risk of concept drift as novel devices, such as, surveillance cameras and personal wearables, which are often unplanned for, are dynamically attached to the smart home automation system. The most sensitive part of smart home automation systems concerns information registry, in this case about the users' energy consumption, from which conclusions about a family's daily routines, life situations, etc., can be drawn, which may form decision support for criminal activities, such as, burglary, stalking, and identity theft.

As an overarching conclusion, the need for a model of security and privacy in the design of smart homes has been defined. It is envisioned as general support for both developers and distributors of smart homes, as well as, the users of them, i.e., for the entire smart home ecosystem. In that sense, the model is also expected to help raise the level of awareness of privacy and security in general IoT-environments, where sensitive user-generated information is an integral part. The main components of this model have been identified in order to address (a) methods supporting the evaluation of risk exposure, (b) security design principles to enable control of the risk exposure, and (c) privacy-aware information

management. However, these challenges are difficult to address if there is no understanding of the information in flux of the smart home, which consequently points to the need for (d) information analysis and classification. An interesting idea is also to (e) integrate security and privacy in the, at least partially, autonomous decision-making process of the connected entities that form the smart home system. In order to address these challenges, it is of course crucial to take into account the specific circumstances regarding both technology and user-interaction that form the smart home environment, i.e., both the user and the technology play central roles.

9. Future work

A general observation is that a more concentrated focus on the development of integrated and automated risk analysis tools that are easy to use is a topic that has not yet been given the attention it deserves. As an example, a systematic and rigorous risk analysis process that includes more analytical aspects, such as, normalization and calibration of evaluations from the evaluators, would be an interesting step forward. With access to such approaches for the analysis of risk and threats in smart home automation systems, an increased understanding of the dangers and hazards that are directed towards systems of hardware, software, users, and information can be enhanced. An adequate comprehension of the risk issues at hand leads to more intelligible and enlightened decision-making processes, especially with regard to choosing and deploying protective measures. Specifically, more research should be put on usable, yet quantitative, risk analysis methods that are based on original and quality data. These methods are needed both on the user and on the developer side, i.e., they should be an integrated part of the design and development process.

Acknowledgments

This work has been carried out within the project "Mobile Services for Energy Efficiency in Existing Buildings", partially funded by Vinnova (Grant No. 2012-01245)—the Swedish Governmental Agency for Innovation Systems. The authors would also like to thank all the members of the project.

References

[1] The Internet of things: Manage the complexity, seize the opportunity, white paper by Oracle, 2014. Available at: http://www.oracle.com/us/solutions/internetofthings/iot-manage-complexity-wp-2193756.pdf (Last checked: 2015-06-02).
[2] S. Björnehaag, Test of a home energy management system at E.ON—an evalutaion of users's expectations and experience (Master thesis), Dept. of Energy Sciences, Lund University, 2012.
[3] A. Fensel, V. Kumar, S.D.K. Tomic, End-user interfaces for energy-efficient semantically enabled smart homes, in: Energy Efficiency, Springer-Business Mediea, Dordrecht, 2014.
[4] S. Radomirovic, Towards a model for security and privacy in the Internet of things, in: Proc. of the First Int'l Workshop on Security of the Internet of Things, 2010.
[5] V. Rickebourg, D. Menga, The smart home concept: Our immediate future, in: 1st Int. Conf. on E-Learning in Industrial Electronics, 2006, pp. 23–28.
[6] T. Denning, T. Kohno, H.M. Levy, Computer security and the modern home, Commun. ACM 56 (1) (2013) 94–103.
[7] A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, Home automation in the wild: Challenges and opportunities, in: Proc. of the ACM Conference on Human Factors in Computing Systems, 2011.
[8] T. Kowatsch, W. Maass, Critical privacy factors of Internet of things services: An empirical investigation with domain experts, in: Knowledge and Technologies in Innovative Information Systems, in: Lecture Notes in Business Information Processing, vol. 129, Springer, Dordrecht, 2012, pp. 200–211.
[9] M. Rozenfeld, The value of privacy—Safeguarding your information in the age of the Internet of everything, The Institute, IEEE, March 7, 2014.
[10] R. Weber, Accountability in the Internet of things, Comput. Law Secur. Rev. 27 (2011) 133–138.
[11] T.R. Peltier, Information Security Risk Analysis, Auerbach Publications, Boca Raton, 2010.
[12] G.W. Hart, Non-intrusive appliance load monitoring, Proc. IEEE 80 (12) (1992) 1870–1891.
[13] M. Weiss, A. Helfenstein, F. Mattern, T. Staake, Leveraging smart meter data to recognize home appliances, in: Proc. of the 10th IEEE Conf. on Pervasive Computing and Communication, 2012.
[14] R. Roman, P. Najera, J. Lopez, Securing the Internet of things, IEEE Comput. 44 (9) (2011) 51–58.
[15] K. Djemme, D.J. Armstrong, M. Krian, M. Jiang, A risk assessment framework and software toolkit for cloud service ecosystems, in: Proc. of the 2nd Int. Conf. on Cloud Computing, GRIDs, and Visualization, 2011.
[16] T. Kirkham, D. Armstrong, K. Djermame, M. Jiang, Risk driven smart home resource management using cloud services, Future Gener. Comput. Syst. 38 (2013) 13–22.
[17] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for Internet of things (IoT), in: Int. Conf. on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, 2011.
[18] H. Ning, H. Liu, L.T. Yang, Cyberentity security in the Internet of things, IEEE Comput. 46 (4) (2013) 46–53.
[19] G. Gan, Z. Lu, J. Jiang, Internet of things security analysis, in: IEEE Conf. on Internet Technology and Applications, 2011.
[20] R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, M. Ratto, The Internet of things, in: Proc. of the First Berlin Symposium on Internet and Society, 2011.
[21] C. Lee, L. Zappaterra, K. Choi, H.-A. Choi, Securing smart home: Technologies, security challenges, and security requirements, in: Proc. of the IEEE Conf. on Communications and Network Security, 2014.
[22] S.R. Das, S. Chita, N. Peterson, B.A. Shirazi, M. Bhadkamkar, Home automation and security for mobile devices, in: Int. IEEE Conf. on Pervasive Communities and Service Clouds, 2011.
[23] S. Notra, M. Siddiqi, H.H. Gharakheili, V. Sivaraman, R. Boreli, An experimental study of security and privacy risks with emerging household appliances, in: Proc. of Int. Workshop on Security and Privacy in Machine-to-Machine Communications, 2014.
[24] A. Arabo, I. Brown, F. El-Moussa, Privacy in the age of mobility and smart devices in smart homes, in: Proc. of Int. Conf. on Social Computing, 2012.
[25] D. Kozlov, J. Veijalainen, Y. Ali, Security and privacy threats in IoT architectures, in: Proc. of the 7th Int. Conf. on Body Area Networks, 2012.
[26] C. Wuest, Smart security for today's smart homes: Don't let attackers spoil your christmas, Symantec Offical Blog. Available at: http://www.symantec.com/connect/blogs/smart-security-todays-smart-homes-dont-let-attackers-spoil-your-christmas (Last accessed: 2015-06-02).
[27] D. Barnards-Wills, L. Marinos, S. Portesi, Threat landscape and good practice guide for smart home and converged media, European Union Agency for Network and Information Security, ENISA, 2014.
[28] O. Whitehouse (Ed.), Security of Things: An Implementer's Guide to Cuber-Security for Internet of Thibgs Devices and Beyond, NCC Group Publications, 2014.
[29] Secure by default: Platforms, the National Technical Authority for Information Assurance, UK, 2012.
[30] U. Eklund, C.M. Olsson, M. Ljungblad, Characterising software platforms from an architectural perspective, in: Software Architecture, in: Lecture Notes in Computer Science, vol. 7957, Springer, Berlin, 2013, pp. 344–347.
[31] D.M. Han, J.H. Lim, Design and implementation of smart home energy management systems based on ZigBee, IEEE Trans. Consum. Electron. 56 (3) (2010) 1417–1425.
[32] S.H. Yuang, ZigBee smart home automation systems, in: Wireless Sensor Networks: Principles, Design and Applications, Springer, London, 2014, pp. 263–274.
[33] P. Baronti, P. Pillai, S. Chessa, A. Gotta, Y.F. Hu, Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards, Comput. Commun. 30 (7) (2007).
[34] A. Kailas, V. Cecchi, A. Mukherjee, A survey of communications and networking technologies for energy management in buildings and home automation, J. Comput. Netw. Commun. 2012 (2012).
[35] A. Hornsby, P. Belimpasakis, I. Defee, XMPP-based wireless sensor network and its integration into the extended home environment, in: IEEE 13th Int. Symp. on Consumer Electronics, 2009.
[36] J. Adams, Risk, Routledge, Oxford, 2000.
[37] B. Carlsson, P. Davidsson, A. Jacobsson, S.J. Johansson, J.A. Persson, Security aspects on inter-organizational cooperation using wrapper agents, in: Agent-Based Technologies and Applications for Enterprise Interoperability, in: Lecture Notes in Business Information Processing, vol. 25, Springer, Berlin, 2009, pp. 220–233.

[38] B. Karabacak, I. Sogukpinar, ISRAM: Information security risk analysis method, Comput. Secur. 24 (2005) 147–159.
[39] J. O'Brien, G. Marakas, Management Information Systems, tenth ed., McGraw-Hill, New York, 2010.
[40] R. Anderson, Security Engineering, second ed., John Wiley & Sons, New York, 2008.
[41] C. Dougleris, A. Mitrokotsa, DDoS attacks and defense mechanisms: Classification and state-of-the-art, Comput. Netw. 44 (5) (2004) 643–666.
[42] P. Paganini, Choosing a DDoS mitigation solution … the cloud based approach, Cyber Defense Magazine. Available at: http://www.cyberdefensemagazine.com/choosing-a-ddos-mitigation-solution-the-cloud-based-approach/#sthash.XIwsFI8a.dpbs (Last checked: 2015-06-02).

Andreas Jacobsson (b. 1977), Assistant Professor in Computer Science at Malmö University. Jacobsson received his Ph.D. in Computer Science in 2008 at Blekinge Institute of Technology in Sweden. His research interests include the theory and application of information security in Internet-based information systems. The results of this work have been published in more than 30 peer-reviewed scientific articles published in international books, journals and conference proceedings. He is a member of the Internet of Things and People Research Center at Malmö University. He is also the Dean of Education at the Faculty of Technology and Society at his University.

Martin Boldt (b. 1977), Assistant Professor in Computer Science at Blekinge Institute of Technology. He received his Ph.D. in Computer Science in 2010 at Blekinge Institute of Technology in Sweden. His research interests include information security, privacy, and data mining. The results of this work have been published in numerous peer-reviewed scientific articles published in international books, journals, and conference proceedings.

Bengt Carlsson (b. 1951), Professor in Computer Science at Blekinge Institute of Technology. His doctoral thesis concerned the multi-agent area with a focus on evolutionary and game theoretical models for explaining both competing and cooperating mechanisms within distributed agent systems. Today, he combines education within candidate and master security programs with research and supervising of Ph.D. students. He has more than 50 peer-reviewed scientific articles published in international books, journals and conference proceedings. The main recent research areas are privacy within information ecosystems, security within virtual companies, malware behavior/prevention and analysis of software in commercial use.