Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home

Jason R.C. Nurse[†], Ahmad Atamli, and Andrew Martin

Department of Computer Science,
University of Oxford, Oxford, UK
[†]`jason.nurse@cs.ox.ac.uk`

Abstract. The Internet-of-Things (IoT) ushers in a new age where the variety and amount of connected, smart devices present in the home is set to increase substantially. While these bring several advantages in terms of convenience and assisted living, security and privacy risks are also a concern. In this article, we consider this risk problem from the perspective of technology *users* in the smart home, and set out to provide a usable framework for modelling security and privacy risks. The novelty of this work is in its emphasis on supplying a simplified risk assessment approach, complete with typical smart home use cases, home devices, IoT threat and attack models, and potential security controls. The intention is for this framework and the supporting tool interface to be used by actual home users interested in understanding and managing the risks in their smart home environments.

Key words: Risk modelling; internet-of-things; smart homes; risk communication; usable security; smart cities; tool support

1 Introduction

Technology has had an enormous impact on our world today. Amongst other things, it has greatly advanced commerce, healthcare, travel, and office and home life. The Internet-of-Things (IoT) is the next significant paradigm set to progress technology even further. It describes a reality where every day 'things' are all connected, working together towards some grander purpose. As the popularity of IoT has grown, so too has the focus on maintaining security and privacy. There have been various articles reflecting on these properties across several IoT contexts, some emphasising their need (e.g., via susceptible vulnerabilities and attacks) and open issues, and others proposing potential solutions for current and future challenges [1]. While these are excellent points of reference, their detail and perspective make them somewhat difficult to apply and use when engaging in practical security tasks, such as risk analysis. Here, we refer especially to cases where one wishes to use such topical reference points along with other information (e.g., network setups) to model the risk in a particular IoT deployment. Moreover, to engage with, and communicate that security or privacy risk to others, for instance, typical users in that environment.

2   Nurse et al.

In this paper therefore, we aim to outline a framework, supported by a prototype interface, to allow the modelling and analysis of the security and privacy risks in IoT deployments; this framework builds on and seeks to apply previous research including our own [1, 2]. A central goal of the framework is to be usable, that is, to provide a simple and intuitive way for common users of IoT technology to model the risks they may face. We scope this work especially to the context of smart homes (i.e., homes with deployed IoT devices) for two reasons. First, the prevalence of, therefore risk faced by, these homes is set to drastically increase in the future, motivated by governments (e.g., smart meters in the UK), supported living (e.g., health-related devices), and convenience (e.g., smart locks and lights). Secondly, we believe there is great value in providing a usable framework that can potentially be employed by a variety of individuals (including non-experts) to have some abstract model of the risks they may face in using IoT at home. This could even assist with issues of risk awareness (as outlined in [3]) in that environment.

To achieve the goals mentioned above, this paper is structured as follows. Section 2 will reflect on the research conducted on the smart home generally, and then from a security and privacy risk perspective. This will help to form an understanding of the current state of the art and highlight key challenges to achieving security and privacy in the smart home. Section 3 presents the core contribution of the article, i.e., the framework. Here, we motivate the need for such a framework, and introduce the modelling process which defines its. We further explain the context where it may be best used, the risk management foundation on which it is based, and the key features likely to increase its usability. Next, in Section 4, we apply the framework to a home scenario to exemplify how it can be used. This section also demonstrates the interface that can support individuals in the actual application task. Section 5 reflects on the framework and its goals, also considering the first impressions of prospective users; this is the important step of framework refinement. Finally, we conclude and present the next steps in this work in Section 6.

2 The smart home and its security and privacy risks

Research on smart cities and smart homes has been under way since the conception of the IoT itself. While smart cities tend to be directly driven by governments and corporations (e.g., smart grids, transport and waste collection), smart homes represent a domain where public consumers have great choice and flexibility. Early research on smart homes sought to digitally engineer home life by proposing sets of adapted appliances likely to be useful [4]. These included smart pens, wardrobes, sofas, refrigerators and windows. Since that work, research in this space has specialised, and can be split into three key areas: home automation, home monitoring and security, and assisted living.

Home automation focuses on streamlined control of home devices such as adaptive lighting, heating and appliances. Whilst industry has aimed to produce clearly defined products, such as the Google Nest thermostat, Belkin's WeMo

range, and Phillips Hue smart lights, research has sought to consider the full range of systems that could be implemented in the home. For instance, Han et al. [5] propose a home energy system design, using popular IoT protocols IEEE 802.15.4 and ZigBee, to provide intelligent services to home users. This includes a multi-sensing, heating and air-conditioning system and actuation application.

The domain of Home monitoring and security emphasises safety and security as key aspects in the home. Products available in this domain include WiFi cameras, motion detectors and smart door locks. Within research, some of the more noteworthy developments span smart home surveillance systems (e.g., proposals for intelligent, real-time remote monitoring tools [6]) to smart door locks with added security (e.g., two factor authentication smart lock solutions [7]). In particular, there has been a good stream of research in terms of assisted living technologies for the smart home. These aim to support individuals, such as the elderly or disabled, in a range of tasks [8].

With such a variety of technology now available for, and present in the smart home, individuals are increasingly at risk. For instance, smart locks meant to authenticate only individuals carrying certain pre-allowed devices, may fail (or be hacked remotely) thus resulting in authorised access to home properties. Moreover, as we have seen in the news, smart fridges have already been used to launch spam attacks [9], and smart TVs may be compromised to allow an attacker full remote control and access to the TV's camera and microphone [10]. Risks relating to security, privacy and dependability of smart home setups has been considered broadly in research, such as Brush et al. [11] and industry, in Kaspersky Labs [12]. While the research article highlights the issues and risks that home users face with these smart devices, the second reports on a more practical assessment of smart home devices and the serious risks that were uncovered (e.g., exposure of passwords and remote device control). These are two of the many articles discussing the range of risks facing the smart home.

In response to the risks, numerous proposals have surfaced. Busnel and Giroux [13] for example, propose a solution that uses security patterns applied to the smart home. A privacy framework is outlined in other work that seeks to support mobile health and home-care systems [14]. Furthermore, research has considered how the cloud service management principles of risk and contextualization can help solve the challenges of emerging smart home devices [15].

One area that has not received much focus however, is that of engaging with the individuals in the smart home on the risks they face through the use of smart home technology devices. This is a subtly different problem to that which is covered in existing research (e.g., [16]) on the usability of security aspects in smart home devices. This is because it is more interested in enabling users to gain an abstract model of the risks that may be present in the use of IoT in their homes. Kumar et al. propose an approach somewhat similar to this with their technique to visualise digital home safety, however, the extent to which users are involved in the process and understand the risk output presented is not clear [17]. We believe that this is a key part of research yet to be tackled and hence why we aim to explore it in this paper.

4   Nurse et al.

3 Framework to support risk modelling in the smart home

A key goal our framework is to keep users in loop with regards to the security and privacy risks of smart home technologies. We appreciate that this is not a task all users will be interested in, however, for those non-experts in the home that are and have basic security and privacy knowledge, this framework could be especially useful. The framework consists of a process to model risks that draws inspiration from several risk assessment approaches [18]. As risk management and assessment are established fields with clear process and structure, we do not seek to replace them, but rather to provide thin layer between such techniques and users that could allow them to better appreciate the threats, attacks and related risks of using these home devices. Figure 1 shows our high-level modelling approach, with five tasks for home users to follow. These are **Use case definition, Assets and network analysis, Threat and attack analysis, Risk definition and prioritisation**, and **Control definition and alignment**.

Fig. 1. An overview of the framework process to model risks

In detail, the **Use case definition** task seeks to get users thinking about the scenarios or uses of the IoT devices in the home. This could adopt a high level or a specific usage perspective. To assist users, our approach relies on a support structure based on simple questions and the provision of several examples (or question answers) at each task level. For this level, the fundamental questions that would be placed to users are: *What scenario(s) or function(s) are the smart/IoT devices intended to support? Who are the individuals in such scenarios?* For guidance in answering these questions, there are a number of use cases with typical home users and relevant stakeholders accompanying the framework that can be referenced or selected directly. For instance, two broad use cases are Smart kitchen automation and complete Home surveillance, whilst specific cases range from Smart home security deployment to using Smart lighting. Of course, users may also decide to choose the most general use case, i.e., Smart home, and indeed we suggest this the first time the framework is applied to a smart home. Once the use cases of interest are identified, they are used to guide later tasks.

Asset and network analysis is the next task for the home user, and involves them defining the devices (assets) that are needed for the use case in focus. Additionally, here we aim to get users think about whether, and potentially how, those devices may communicate with each other to achieve their functions; this will be important in subsequent risk modelling tasks. The respective questions presented to users are: *What are the smart/IoT devices or products that support the use case? How do these devices connect or work together (or simply, what communicates with what)?*

To support individuals, the framework lists sets of devices typically used in the home, including smart TVs, door locks, alarms, lighting, thermostats, fridges, kettles, motion sensors, smoke detections, cameras, and hubs. Upon selecting relevant devices, users are asked to connect devices that may interact with each other. For instance, assuming the Smart door lock case, the devices used may include the smart lock and any smart phones that connect to it. The communication definition would include links from each smart phone to the smart lock (vendor specific app on the smart phone would define communication specifics); these are ad hoc networks, and scoped only to this use case. If the home user was interested in mapping the entire Smart home or the Smart home security features, they would also need to consider all the other devices linked to the smart phone, such as routers, PCs and other smart devices.

During this task, home users are also asked to prioritise the various IoT devices identified. Two questions that the framework poses to assist individuals are: *On which devices do the more sensitive data reside? What devices might result in the greatest harm if they were compromised (or failed to work as expected)?* Users can select from the smart devices identified earlier, and annotate them with priority details. Given the variety of users in the home, we suspect that many may not have a good understanding of the most important devices according to the questions above. To support this activity, aspects that may be relevant are listed with each device in the framework's catalogue. Therefore, for a smart TV, its microphone and camera, in addition to the fact that it may be used to enter account credentials (e.g., Amazon) or indeed, bank details for paid TV, could cause it to be considered as more important than an average device.

To keep the prioritisation simple whilst remaining useful, three stepped Likert scale levels are suggested for rating; Very important (e.g., device contains sensitive personal data such as bank details or social security numbers, or, the device allows full physical / remote access to the home), Moderately important, and Not that important (e.g., compromise of the device has little to no impact on the home or individuals in it).

With the assets and ad hoc networks identified, we then move to the **Threat and attack analysis**. The goal in this task is to define relevant threats, or specifically threat actors and map them to attacks. The question here is: *Who might seek to harm or compromise devices or individuals in the home?* Threat actors in this context are individuals that perpetrate attacks on the smart home. While there are an extensive set of actors that may be considered (both in terms of motive and capability), for ease of use the framework's initial list consists of Hackers (online), Criminals (offline), and Stakeholders / Users (Malicious/Intentional or Unintentional). The next step is to consider and link the attacks that such actors may launch, therefore; *how may the network (or part thereof) be harmed or compromised?* We support home users in this by drawing on our previous work [2]. In that research, we identify, describe and give comprehensive examples of the main types of attack on IoT devices, namely, device tampering, information disclosure, privacy breach, denial-of-service (DoS), identity spoofing, elevation of privilege, signal injection, and side-channel attacks. In addition to this, the

6   Nurse et al.

framework provides examples of how certain threat actors may launch attacks. For instance, a hacker might conduct a DoS attack against a home router from the Internet, or a burglar may use an infected smart phone to tamper with a smart door lock. We note here that a glossary of all the security and risk terms is available with the framework.

In the **Risk definition and prioritisation** task, the framework combines output from previous tasks and aims to get users thinking about how at risk are the various home devices. Key questions here are: *What is the impact on an asset of an attack, or simply, what do home users stand to lose? How likely is the attack to occur?* For both of these, users can choose options on a likert scale from 1–3 in terms of impact and likelihood. For users, the framework highlights that level of impact can be linked to the importance levels highlighted before for assets. Therefore, if a criminal manages to compromise a front door smart lock, then the impact is very significant given they then have full access to the house. Similar to more formal risk assessment applications, likelihood is more difficult to estimate. For this, we suggest using knowledge of the number and type of individuals that may have access to the home, the neighbourhood of the home itself, and any previous attack (online or offline) information. For example, in a smart home where there are carers visiting daily to tend to the elderly, there may be an increased likelihood of device tampering (directly) or information disclosure (if they mistakenly connect an infected device to the home network).

To actually define the risk, the framework adopts a traditional approach of combining the impact and likelihood scores for attacks [18]. Therefore, for a device tampering attack on a smart lock, the impact might be very significant (3) considering what harm could result, but not likely (1) given the individuals live in a gated area. Using the straightforward metric of multiplication, the risk score would be 3 (out of a possible 9). As each attack related to the use case in focus is rated, the result would be a list of risks and respective scores. We appreciate that risks may be best perceived and interpreted in different ways [19], and therefore in addition to numeric scores also seek to use visual and verbal messages according to the score values. At present, we apply simple visuals based on colours, red, amber and green (for the main categories of high, medium and low risk); with wording such as 'These risks represent a serious area of concern for the smart home (for High risks)' also available. A future option for visuals is to integrate risk iconography [20] in the hope of being more accessible to users.

Whilst modelling risks will allow individuals to gain insight into areas of potential concern in their smart homes, it would be prudent to also supply guidance on the management of such risks. The **Control definition and alignment** task serves this purpose, by allowing home users to ask the framework: *What security controls may be applied to address the risks?* There are several different security controls that may be applied to address the various types of risk (and underlying attacks). To assist home users in identifying relevant controls, the framework draws on the OWASP Consumer IoT Security Guidance documentation [21] and aims to automatically link the guidance categories to the identified attacks. These categories outline approaches to address insecure web interfaces,

physical security of devices, network services security and privacy concerns. For example, to address risks pertaining to insecure web interfaces and attacks such as identity spoofing or information disclosure, guidance is given on applying two factor authentication and engaging in network segmentation (e.g., using firewalls to segment critical devices). This process also allows users to witness how controls align to the risks present.

4 Applying the framework

To apply the framework, users have the option of a prototype support tool, or a more manual approach using the documentation provided with each task. In this section, we describe aspects of the tool in particular, along with a simple example of its application to a risk modelling scenario. The scenario is one where a home user has installed a smart door lock to control access to their house. To commence modelling, users open the tool and create a new project. From there, they are directed to an interface for Task 1, i.e., Use case definition. In Fig. 2 we present two screenshots of the Task 1 interface.
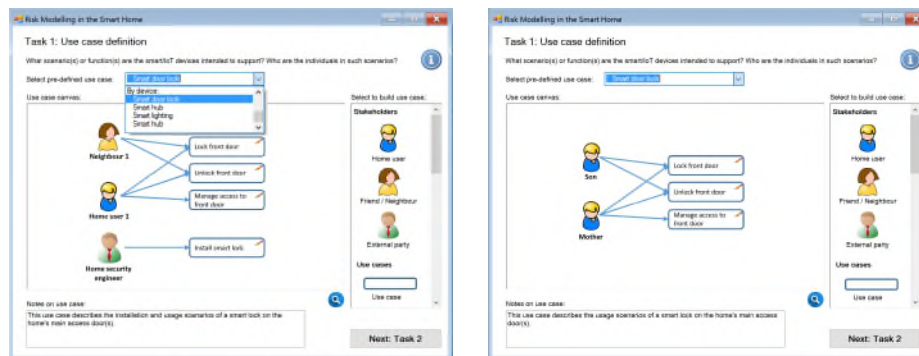

Fig. 2. Task 1 Risk modelling tool interface. The interface allows users to draw on predefined use cases, whilst also providing the graphical modelling, annotation and information-support capabilities to craft their own cases (by simple drag and drop).

As mentioned in Section 3 and shown in Fig. 2, users are first presented with questions setup to guiding the task. They can either select from the set predefined use cases (in the dropdown list depicted), or directly create their own by choosing relevant template items (users or use cases) from the scrollable list to the right of each interface screen. Given this scenario is similar to one in the predefined set, the user decided to select it to begin modelling. Selection automatically populates the Use case canvas (a user-editable area) centre screen with graphically depicted related scenarios and adds preliminary notes.

The scenarios added are not necessarily intended to be used as they are, but instead should (a) help users think about other pertinent individuals and activities (e.g., a home security engineer or device installation), and (b) be modified

8   Nurse et al.

to suit specific new cases. Therefore, the system then prompts users to update the selected cases; they can rearrange, delete or add new items to the canvas as desired. In this instance, the user has modified the initial case, and created a more relevant one (with a mother and son in the home, and no other individuals involved with setup or possessing access) shown to the right of Fig. 2. If users require help or further information to assist in this task, there is an information icon in the top right of every screen.

In the Asset and network analysis task, users are presented with a similar structural interface to that in Task 1: with relevant questions and predefined IoT device options at the top, a list of device options to the right, a canvas in the middle, places to add notes, and information points. Given that the Smart lock use case was selected in Task 1, the system automatically populates Task 2's canvas with a Smart lock and two smart phones (one for each user), and creates a connection from the phones to the lock. Users are then requested to edit the canvas as necessary, to consider on which devices sensitive data resides, and what devices may lead to the greatest harm if compromised. The tool helps users by presenting potential aspects (e.g., credentials on smartphones and failure of the lock to allow entry) that may be relevant alongside each device icon shown. Annotations are added to the icons in the canvas by double clicking them; this also includes the 1–3 impact ratings.

The Threat and attack analysis task is next and involves using the tool to model relevant threat actors and attacks on IoT devices in the home. Support in this task is in the form of automated examples tailored to the previously identified IoT devices (assets) and the home's main users and stakeholders. Some of these examples are presented in Fig. 3.
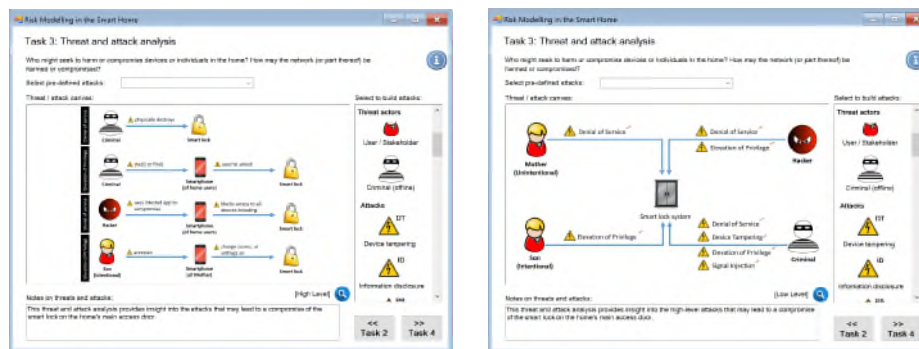

Fig. 3. Task 3 Risk modelling tool interface. This interface explores, in varying levels of detail, the threats and attacks facing the smart home.

In the screenshot to the left of Fig. 3, there are examples of preset attacks from the framework's catalogue which users can customise as they desire. For instance, a criminal could physically destroy a smart lock, potentially preventing other legitimate users from accessing it. There is also the fact that individuals

without management level access (e.g., the 'Son' in this case) may use their trusted position to further elevate their or other individuals' privileges. Most importantly, these examples should give users some initial insight into the attacks they may face. As with previous tool interfaces, they can use the items (here, threat actors, attacks and IoT devices) on the right, to edit or compose additional attacks shown on the main canvas. To the right of Fig. 3, the high-level, summary of attacks, threat actors and the IoT system is presented; this is intended to be a simplified version of the low-level interface (to the left). Users can toggle between these interfaces using the 'High Level' or 'Low Level' options next to the zoom button below the canvas.

A central aim of the framework is to allow its users to better understand and model the risks which they face through the use of smart devices in the home. The Risk definition and prioritisation task is central to this. The tool's usage here is to combine user input and models previously supplied, and enable users to add further data about attack likelihood and impact to appropriately characterise the risk. This is achieved through a series of prompts for user input, where the tool asks for estimates regarding these aspects; while limited support is provided here, the tool does remind users of assets that were previously highly prioritised, as the impact on these if compromised may be greater. The result of entering this data is a Risk report; an example of which is shown in Fig. 4.
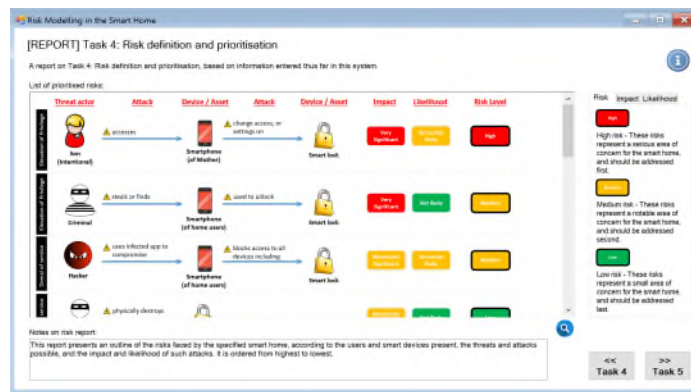

Fig. 4. Task 4 Risk report listing the risks facing the defined use case.

A Risk report is a list of risks, ordered in terms of their overall rating. As shown in our running example in Fig. 4, the risks along with their corresponding impact and likelihood ratings are expressed as an extension of each attack. This allows the individual modelling the risks or a user wishing to communicate those risks to others, to easily track their origin and related threat actors, whilst also viewing other attack details. To support an accessible and accurate perception and interpretation of risks, we use a combination of visual and verbal messages, with colours and descriptions for risks (including impact and likelihood) [19]. Moreover, to enable users to quickly spot the most serious risks facing the use

10   Nurse et al.

cases they initially identified, the system automatically orders risks by their levels. Given that this is a report, users are not able to edit it, but as necessary they can use the "<< Task 4" button to return to the previous screen.

The final task is Control definition and alignment. Here, the system draws on predefined mappings between attacks and respective countermeasures to suggest an initial set of security controls for the home users to consider. As highlighted prior, these controls are based on the OWASP Consumer IoT Security Guidance documentation [21]. The central tool interface is similar to Fig. 4, except for the fact that it is editable and if relevant controls have been identified for risks, they are listed next to each risk. For instance, consider the highest rated risk in Fig. 4 which involves elevation of privileges through accessing a privileged smart / mobile device. The related OWASP guidance category is 'I7: Insecure Mobile Interface', and therefore, some of the control options that would be suggested include: requiring a PIN or password; using two factor authentication (even biometrics, given its increased prevalence in smart phones); and enabling account lockout functionality. Users can decide which option(s) they wish to implement and add notes in the system if they desire. To facilitate sharing of the risk models developed in the tool, an export function is available which presents models similar to their representation in the interface.

5 Reflection on framework and users' first impressions

The aim of this research was to provide a framework and supporting prototype interface to allow the modelling and analysis of the security and privacy risks in smart home deployments. We achieved this aim by considering the key components of risk analyses. In developing this framework, making the security and risk management process usable and accessible was a critical goal. This, we believe, could make understanding the risks with new smart devices much more tangible, thus potentially result in more proactive security behaviour. To achieve this, we built the framework to provide simplified guidance in the risk assessment process, and support via several predefined aspects (e.g., attacks, threats). Further support was available in a tool prototype that home users could follow the main five tasks, and model their own households and risks they face. We designed the prototype with security usability guidelines in mind, especially to be accessible, while still ascribing to the main activities in general risk management [22].

Although we believe that this is a good start at addressing a notable and increasingly relevant gap in smart home research and practice, further work needed both on the framework and prototype. One challenge yet to be tackled for example, is that whilst the abstract modelling of risks and attacks possible with the framework could help understanding, without consideration of specific vulnerabilities in different smart devices, the analysis is arguably limited. How we capture and include this information, and present it in a way that is still accessible to home users is a question for future research. A related challenge is in the mapping of security controls to risks and attacks – a high-level mapping can offer value especially for some types of users, but specific knowledge of attack details (possibly at the CAPEC level) may lead to better mappings of controls.

To gather some preliminary feedback on our framework and tool interface, we conducted informal interviews with five home technology users. The interviews involved explaining the purpose of the framework, demonstrating how it could be used, and then allowing them to apply it to any scenario they desired and ask questions. Overall, most users were able to quickly adopt the process, and they found the visual interface and support features (e.g., selection lists, automatic mapping) useful. We did notice a few issues in the framework usage however. For instance: (i) the way users modelled and linked assets, threats and attacks was not always logical or correct – e.g., a criminal stealing sensitive data from a smart light; (ii) users often disagreed on what devices should (and should not) be included in a particular use case risk assessment; and (iii) users felt that for complex use cases with a variety of home devices, the interface may not scale well. Respective resulting issues that will need to be addressed therefore include: (i) allowing flexibility but also introducing feasibility constraints on models; (ii) reviewing the pros and cons to scoping case and risk models; and (iii) testing the tool's ability to scale, and potential enhancement of interface designs. These are all aspects to be used to guide our future research.

6 Conclusion and future work

As technology continues to permeate the home, home users are facing a significant number of new security and privacy risks. This research aimed to provide them with some insight into those risks, via the definition of a risk modelling framework and supporting tool interface. We sought to frame these approaches as a simple and intuitive way for users of IoT technology to model the risks they may face in the home context. We also applied and reflected on our work, and highlighted some key first impressions from prospective users. These reflections identified some of the main aspects which we will seek to tackle in future work. Particularly, the question of how to include the appropriate level of detail so that our tool is highly usable and scales well, but still supplies home users with the information they need to make good security decisions. Once our next iteration of design and development is complete, we will conduct more detailed user testing to evaluate the real utility of our proposal.

References

1. Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A.: Security, privacy and trust in internet of things: The road ahead. Computer Networks **76** (2015) 146–164
2. Atamli, A., Martin, A.: Threat-based security analysis for the internet of things. In: International Workshop on Secure Internet of Things (SIoT), IEEE (2014) 35–43
3. Caviglione, L., Lalande, J.F., Mazurczyk, W., Wendzel, S.: Analysis of human awareness of security and privacy threats in smart environments. In Tryfonas, T., Askoxylakis, I., eds.: Human Aspects of Information Security, Privacy, and Trust. Volume 9190 of Lecture Notes in Computer Science. Springer (2015) 165–177
4. Park, S.H., Won, S.H., Lee, J.B., Kim, S.W.: Smart home–digitally engineered domestic life. Personal and Ubiquitous Computing **7**(3-4) (2003) 189–196

12   Nurse et al.

5. Han, D.M., Lim, J.H.: Smart home energy management system using ieee 802.15. 4 and zigbee. Consumer Electronics, IEEE Transactions on **56**(3) (2010) 1403–1410

6. Hou, J., Wu, C., Yuan, Z., Tan, J., Wang, Q., Zhou, Y.: Research of intelligent home security surveillance system based on zigbee. In: International Symposium on Intelligent Information Technology Application, IEEE (2008) 554–557

7. Priyadharshini, S., Nivetha, D., Anjalikumari, T., Prakash, P.: Mobile controlled door locking system with two-factor authentication. In: Proceedings of the International Conference on Soft Computing Systems, Springer (2016) 133–139

8. Arcelus, A., Jones, M.H., Goubran, R., Knoefel, F.: Integration of smart home technologies in a health monitoring system for the elderly. In: 21st International Conference on Advanced Information Networking and Applications, IEEE (2007)

9. BBC: Fridge sends spam emails as attack hits smart gadgets (2014) http://www.bbc.co.uk/news/technology-25780908.

10. Michéle, B., Karpow, A.: Watch and be watched: Compromising all smart TV generations. In: Consumer Communications and Networking Conference. (2014)

11. Brush, A., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., Dixon, C.: Home automation in the wild: challenges and opportunities. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM (2011) 2115–2124

12. Kaspersky Lab: Surviving in the IoT world: Kaspersky Lab Experts Discover the Risks of Smart Home Devices (2015) http://www.kaspersky.com/about/news/press/2015/Surviving-in-the-IoT-world-Kaspersky-Lab-Experts-Discover-the-Risks-of-Smart-Home-Devices.

13. Busnel, P., Giroux, S.: Security, privacy, and dependability in smart homes: a pattern catalog approach. In: Aging Friendly Technology for Health and Independence. Springer (2010) 24–31

14. Kotz, D., Avancha, S., Baxi, A.: A privacy framework for mobile health and home-care systems. In: Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems, ACM (2009) 1–12

15. Kirkham, T., Armstrong, D., Djemame, K., Jiang, M.: Risk driven smart home resource management using cloud services. Future Generation Computer Systems **38** (2014) 13–22

16. Kalofonos, D.N., Shakhshir, S.: Intuisec: a framework for intuitive user interaction with smart home security using mobile devices. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, IEEE (2007)

17. Kumar, P., Subramanian, N., Zhang, K.: SaViT: Technique for visualization of digital home safety. In: 8th IEEE/ACIS International Conference on Computer and Information Science, IEEE (2009) 1120–1125

18. NIST: Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems (2010)

19. Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K.: Trustworthy and effective communication of cybersecurity risks: A review. In: Socio-Technical Aspects in Security and Trust Workshop at the Network and System Security (NSS) Conference, IEEE (2011) 60–68

20. Hosmer, H.H.: Visualizing risks: Icons for information attack scenarios. Technical report, DTIC Document (2000)

21. OWASP: Consumer IoT Security Guidance (2015) https://www.owasp.org/index.php/IoT_Security_Guidance.

22. Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: Past and present. In: Cyberspace Safety and Security Workshop at the Network and System Security (NSS) Conference, IEEE (2011) 21–26