An IOT Security Awareness and System Hardening Advisory Platform for Smart Home Devices

Aimee Shepherd and Edward Apeh

Faculty of Science and Technology, Bournemouth University, Poole, United Kingdom

s5001169[1], eapeh[2] @bournemouth.ac.uk

Abstract. This poster will demonstrate the work currently being undertaken to develop the proposed platform for IoT Security and System Hardening Advisory. It will highlight the current state of art for IOT security awareness and system hardening advisory. It will also present the investigation into the use of end-user approaches such as crowdsourcing and gamification to facilitate the sharing of security related information on SMART home devices within a community of end-users, retailers and manufacturers. Also, it will present the design of the experiments to evaluate the proposed platform's performance in engaging its users and its provisioning of a continuous feedback loop of identification and recommended resolution of SMART home devices security issues.

Keywords: Internet of Things, Smart Home Devices, End User Engagement

1 Introduction

The recent proliferation and dependence on SMART home devices has resulted in a corresponding increase in evolving threats and attacks on the IOT devices that makeup the SMART home. There is therefore a clear need for providing continuous up to date threat information and hardening recommendations for smart devices from off the shelf to end of life.

Figure 1 highlights a direct correlation with the rise of installed bases to the rise of different attack vectors with, for instance, a 40% surge in global ransomware, 19% increase in intrusion attempts, and 30% rise in IoT malware. [2]

This extended poster abstract will present the work currently being undertaken to develop an IOT security awareness and system hardening advisory platform for smart home devices. It highlights the current state of art for IOT security awareness and system hardening advisory. It presents the investigation into the use of end-user approaches such as crowdsourcing and gamification to facilitate the sharing of security related information on SMART home devices within a community of end-users, retailers and manufacturers. Finally, the poster presents the design of the experiment to evaluate the proposed platform's performance in engaging its users and its provisioning of a continuous feedback loop of identification and recommended resolution of SMART home devices security issues.

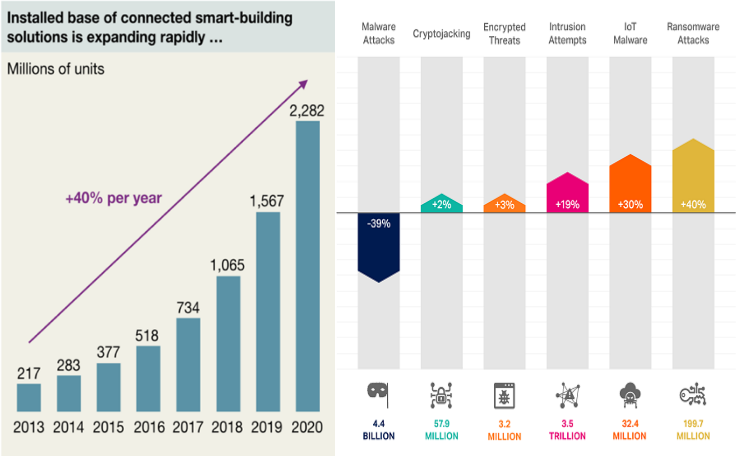

Fig. 1. A side-by-side illustration of the rapid expansion of smart building solutions over 7 years alongside the increase in the attacks on smart home IOT devices. [1]

2 Background Information

Smart home systems include a wide range of mobile and/or web solutions for monitoring, controlling and automating functions in the home.

The connected IOT devices that make up smart home systems (i.e. Internet-connected "thing" ranging from power grids to smart doorbells) is set to be 41.6 billion by 2025. This increase in IOT devices has been matched by an increase in the number and sophistication of IOT device attacks over time as shown in Figure 2. [3]

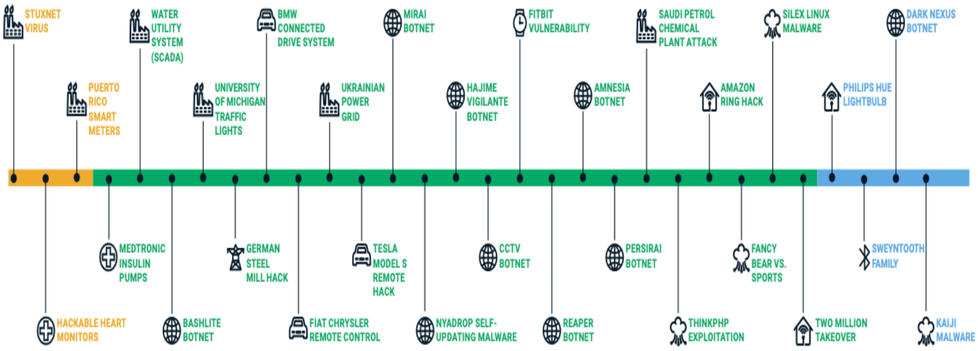

Fig. 2. A timeline of attacks and exploitations on IoT.

Most attacks on smart home systems tend to take advantage of the out-of-the box default settings on smart home systems. Furthermore, threat actors have also exploited the non-technical awareness of end-users. As more consumers adopt IoT solutions in the home, their role in the overall security and privacy of IoT increases. Consumers are also required therefore, to take a more active role in purchasing and in their home security and privacy.

In addition, competition and pressure to bring products to market results in shortcuts taken during the manufacturing and design processes. A recent report by GOV UK has highlighted that one of the key factors influencing the level of cyber security, or lack thereof, in consumer IoT devices is a lack of consumer awareness of what to look for in a device to ensure it is secure. Furthermore, the report highlighted how without a unified standard to mark a device’s security level, consumers have no clear way of determining whether the device they have purchased will protect their data. [4] Whilst there is a limited number of materials available for end users, such as the NCSC’s one pager on how to purchase secure IoT devices, they do not provide a place where consumers can understand their devices security level and the reasoning behind it. [6]

Along with a general lack of awareness of the threat posed to IOT devices, there is a lack of physical hardening is a key impact on the rise of IoT attacks [5]. These have all combined to increase the attacks and severity on the IOT devices that make up the smart home system. The proposed solution aims to provide a system to improve the lack of hardening and awareness for not only consumers but also manufacturers and retailers.

A survey conducted by the IT security firm Trend Micro has revealed that 86% of IT and security decision makers around the world believe their organisations need to enhance their awareness of IoT Threats. [2]

This statistic demonstrates clearly the need for a solution for all users of IoT devices, inside the organisations and outside.

The eight most common vulnerabilities in IoT devices named by OWASP include insecure network services, lack of secure update mechanisms and the lack of physical hardening. Hackers actively exploit weaknesses in IoT security not to attack the devices themselves, but as a point for all kinds of malicious behavior. Such as, DoS attacks, malware distribution, spamming/phishing, click fraud, credit card theft. [4]

The proposed solution will allow for the eight most common vulnerabilities to become more publicly aware by end users of smart home devices and also advise them on how they can harden their devices, to further protect them from potential threat actors.

3 Current Solutions and their Shortcomings

Existing approaches to address the lack of awareness and advisory of the evolving threats posed by smart home devices tend to range from bug bounty programmes to patch management. These solutions are however limited in their coverage and often miss out on vital input and involvement of non-technical end-users. Furthermore, existing approaches tend to be more reactive than proactive in the detection and resolution of security issues of SMART home devices.

InfraGard a partnership between the FBI and the private sector provides a platform for association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. However, it has very little provision for the engagement and sharing vulnerabilities or issues with the general public. Furthermore, the catch-all nature of the InfraGard platforms makes it challenging to identify SMART home devices threats.

The NCSC have created a platform, working with small to medium sized enterprises, charities, legal and accountancy sectors, as an e-learning training package. The aim is to ensure that staff are staying safe online, it covers areas on why cyber security is important and how attacks happen. Again, a short coming of this is that it is not available publicly and therefore proves there is a gap in the market for the proposed solution which is discussed in the next section.

These existing solutions whilst providing information about cyber threats have very little end user engagement – especially in terms of reporting and feedback provision of IOT device vulnerabilities and threats. The end user is the key actor in how IoT's will shape the future and without their continuous feedback throughout the life of an IoT device, limited improvements will be made. [6]

4 Proposed Solution

To address these shortcomings, an IOT security awareness and system hardening advisory platform for smart home devices is proposed. The proposed platform will incorporate crowdsourced security information from SMART home devices end-user with processed information on SMART home devices vulnerability obtained from CVE and/or NVD. The aim is to curate, analyse and present security issues of SMART home devices along with the relevant recommendations for addressing them to manufacturers, retailers and end-users.

Gamification is the use of video game elements in non-gaming systems to improve user experience and user engagement. [8]

In persuasive technology, video games and game aspects have been studied as potential means to shape user behaviour in directions intended by the system designer or to instill embedded values. The proposed solution aims to in still gamification embedded in the solution as well rewarding users for completing tasks as such, to ensure that the system hardening advisory aspect of this solution is understood and taken on board by end users.

This will allow manufacturers to really reach into each demographic of end user and understand the use and functionality of their devices more ensuring that the market of IoT can become richer and smarter over time.

Crowdsourcing will also be a main aspect of the end user interaction feature of this system. Crowdsourcing is a problem-solving model based on the combination of human and machine computation, it is the act of outsourcing work to an undefined, networked labour using and open call for participation. [9]

The proposed solution will use crowdsourcing in the form of community forums to allow end users, manufacturers and retailers of such devices to communicate open and freely on all topics concerning The Internet of Things and Smart Devices. Table 2 shows the use cases of the proposed solution.

Table 2. Use Cases of the Proposed Solution

	Use Case
Manufacturers and Retailers	Manufacturers will use this system to navigate through the IoT devices that they are interested in and through the feed from the CVE they will discover whether any devices of interest currently have any known vulnerabilities. The system will provide details on how they can advise users to harden their system. Further, they can interact with end users through community forums to engage regarding feedback or any concerns.
End Users	End users will use the system to understand how their smart home devices work and how they can further protect themselves in the home environment whilst using their smart devices to the best of their ability. They will interact with manufacturers and retailers through forums and crowdsourcing to engage regarding feedback, concerns or any issues.

Nelson’s heuristics will be used throughout the project to analyse how the users will interact with this system and requirements will be based on these scenarios. Nelson’s heuristics will be a continual part of the agile evaluation process throughout the entirety of the project lifetime.

Key features of the proposed system will be a feed (determined by CVE entries), either listed by brand or device of the current status of the home device. For example, Amazon’s Alexa will be shown in a user engaging way with pictures and underneath there will be shown its current vulnerability status using a traffic light system. Moreover, the use of gamification will ensure that users find the system ‘fun’ to use and increases the amount of time they spend learning about their smart home devices.

Crowdsourcing will be used to gather feedback and knowledge from end users to further improve future and existing devices.

Further, community forums will be highly encouraged by engaging topic titles to ensure that users feel comfortable using these. These crowdsourcing forums will encourage users to give feedback on the devices they own or are looking to own on any issues or simple recommendations to improve the useability to the manufacturer/retailer.

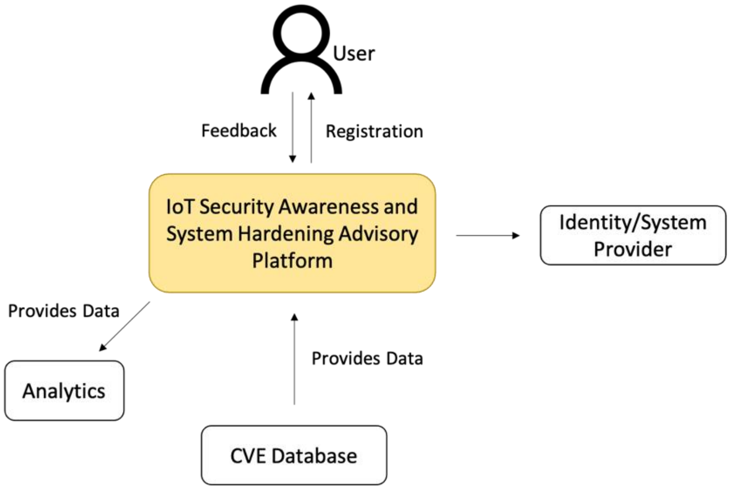

Fig. 3. A context diagram of the proposed solution.

Figure 3 highlights a brief context diagram of the proposed solution. “User” in figure will be defined as all end users, manufacturers and retailers that will use the system.

The key benefits to the proposed solution include:

1. Improved feedback loop – with the use of crowdsourcing and open community forums, end users of smart home devices will have the open space to engage with other users, manufacturers and retailers freely. This aspect is something that hasn’t been seen in terms of IoT devices and therefore it will greatly increase the feedback loop of this market.
2. End user engagement – the use of these crowdsourcing community forums will allow for the end user engagement to increase and also the knowledge of our end users of smart home devices and therefore the whole experience of owning a smart home device increase. End users are more likely to recommend products and services once they understand them more.
3. End user interaction – due to the increase in knowledge about their device, be it security, functionalities or usability, the interaction with smart home devices with inevitably increase. This could mean the purchasing of more devices for their home and greatly increase sales and understanding of IoT devices, consequently increasing the reputation of smart home devices as this sector grows.

4.1 Testing and Evaluation

The system will undergo testing and evaluation with different demographics to ensure that all perspective users of the system will be able to navigate this with ease.

Below in Table 3 you can find a test specification which will be used to conduct the testing once the system has been produced. The caveat to this may be that particular details of the may be adjusted or changed to suit the end results.

Table 3. Test Cases for the Proposed Solution

Test Case	Expected Outcome
User in 18-24 range to navigate the site.	User is able to navigate the site with no problems where each area is clearly signposted, and it is understood the nature of each section of the system. Further, they will have very minimal questions regarding the system in terms of useability and functionality.
User in 25-40 range to navigate the site.	User is able to navigate the site with no problems where each area is clearly signposted, and it is understood the nature of each section of the system. Further, they will have very minimal questions regarding the system in terms of useability and functionality.
User in over 40 range to navigate the site.	User is able to navigate the site with no problems where each area is clearly signposted, and it is understood the nature of each section of the system. Further, they will have very minimal questions regarding the system in terms of useability and functionality.
Corporate manufacturer or retailer to navigate the site.	User is able to navigate the site with no problems where each area is clearly signposted, and it is understood the nature of each section of the system. Further, they will have very minimal questions regarding the system in terms of useability and functionality.
End user to create a new thread in the community forums.	End user is able to navigate freely to the community page where they will easily find the button of how to create a new thread and they are able to conduct themselves through the process of creating the thread with ease.
End user to post in an existing thread.	End user is able to navigate freely to thread in question and is able to post a comment or reply to this thread with ease and minimal questions.
Manufacturer/Retailer to create and reply on a thread.	User is able to navigate freely to thread in question and find the reply section and easily reply to the thread as expected with minimal questions.
Manufacturer/Retailer to push notify an end user of security hardening recommendation.	User is able to navigate to the dashboard where they can push notifications either to a specified thread or new thread, or they can push to all users of the system regarding system hardening advise.
Manufacturer/Retailer to navigate the vulnerabilities to find a particular known vulnerability.	User is able to navigate to the vulnerabilities tab and find the vulnerability in question or view the top 5 vulnerabilities.

After testing has been completed, a review of this will be undertaken to investigate whether the expected outcomes meet the actual outcomes. Moreover, any changes that may be needed will be noted and the system adapted accordingly.

5 Summary and Conclusion

In conclusion, it is apparent that the existing solutions in the area of IoT security awareness and system hardening advisory are not adequate for regular home end users of such devices. Therefore, the proposed solution aims to cover these shortcomings and provide a system which is open sourced and benefits the manufacturers, retailers and end users of these devices. Such, it will ensure that the system is user friendly and tailored to all possible users to further increase engagement.

6 Future Work

Future work of this system will be in the area of gaining a high user engagement with the plan to make the system completely open sourced and free to use.

The main focus will be ensuring the system is easy to navigate for all users and increase the feedback that manufacturers and retailers gain for the smart devices that are already in the market. Further, the use of gamification will be developed to ensure that all learning methods for different personalities are covered for a higher engagement and retention of information.

References

1. Memoori. 2021. *How Many Connected Devices are there now in Smart Buildings?*. [online] Available at: <https://memoori.com/buildings-make-majority-connected-devices-much-building-now-connected/>
2. Prnewswire.com. 2020. *New SonicWall Research Finds Aggressive Growth in Ransomware, Rise in IoT Attacks*. [online] Available at: <https://www.prnewswire.com/news-releases/new-sonicwall-research-finds-aggressive-growth-in-ransomware-rise-in-iot-attacks-301162392.html>
3. Prnewswire.com. 2020. *New SonicWall Research Finds Aggressive Growth in Ransomware, Rise in IoT Attacks*. [online] Available at: <https://www.prnewswire.com/news-releases/new-sonicwall-research-finds-aggressive-growth-in-ransomware-rise-in-iot-attacks-301162392.html>
4. UK, G., 2016. The Cyber Aware Perception Gap. 1st ed. [ebook] UK: GOV UK. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/684609/BT_CYBER_AWARE_V11_280218.pdf>
5. Rentz, P., 2019. *OWASP Releases Latest Top 10 IoT Vulnerabilities*. [online] TechWell. Available at: <https://www.techwell.com/techwell-insights/2019/01/owasp-releases-latest-top-10-iot-vulnerabilities>
6. L, S., 2020. *NCSC's new cyber security training for staff now available*. [online] Ncsc.gov.uk. Available at: <https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available>
7. Federal Bureau of Investigation. 2019. InfraGard | Federal Bureau of Investigation. [online] Available at: <https://www.fbi.gov/about/partnerships/infragard>
8. Webster, M., 2021. Definition of GAMIFICATION. [online] Merriam-webster.com. Available at: <https://www.merriam-webster.com/dictionary/gamification>

9. Webster, M., 2021. Definition of CROWDSOURCING. [online] Merriam-webster.com. Available at: <https://www.merriam-webster.com/dictionary/crowdsourcing>