CyberSDnL: A Roadmap to Cyber Security Device Nutrition Label

Abdullahi Arabo

Computer Science and Creative Technologies
The University of the West of England
Bristol UK
Email: abdullahi.arabo@uwe.ac.uk

***Abstract*—Security issues mainly evolve from attacking the weakest link within the chain of the ecosystem. One of such weakest links with poor security posture is the smart devices used within a smart space and as Bring Your Own Device (BOYD) for the corporate sector. The main focus of this paper is to briefly highlight the issues and present a roadmap that will facilitate better cyber security footings for smart spaces ecosystems. Based on our findings, we have also proposed a Cyber Security Device nutrition Label (CyberSDnL) conceptual framework as a contribution to the knowledge within this field. Our contributions are threefold: 1) inform the user of the risk associated with their device; this is also a crucial requirement for organization in reference to the development of the new General Data Protection Regulation (GDPR) 2) try to influence manufacturers to change their attitudes towards producing unsecured devices and 3) use this as a platform to create early warning systems to the ecosystem that will be able to stop already infected/insecure devices from proliferating vulnerabilities or risking the entire network/ecosystem from an attack.**

Keywords–smart device security; privacy; cyber security; security labels; moving target defense.

I. INTRODUCTION

Communications technologies, devices, and services are becoming more interconnected; hence an enabled future Internet of Things (IoT) connected home. Even though this development offers extensive assistance to home users, it also gives rise to new security threats as this device act as a means of data crowd-sensing agents. The development of ubiquitous computing; IoT to be more specific, has empowered the concept of a connected home ecosystem. This notion is around content anywhere, crowd-sensing and information sharing. Use of IoT devices within connected home ecosystems spawns a cumulative volume of data, habitually lacking the assent of the user, or the user being absolutely cognisant of the insinuations of partaking their personal data. This paper provides a new and easy to use security framework for home devices, with the aim of minimizing the security and privacy threats identified.

Arguably the Internet is one of the utmost human successes in terms of inter-connectivity of things and general telecommunication. However, the development of connected home ecosystems as a result of ubiquitous computing and IoT, promises to make things even more challenging in terms of security and offers more possibilities for improving our way of lives. As a result, users are demanding for seamless inter-connectivity of things to offer countless capabilities to users within their homes and offices. This development is a welcome development, nonetheless, it needs to be noted that it opens up more security and privacy issues for users and critical infrastructure. While we have knowledge of some of the possible vulnerabilities, that are normally only associated with traditional infrastructures, there has been little research and into the individual privacy matters as a result of an interconnected system where devices, with various level of complexity and security, exchange information via a wireless connection to the Internet. Interconnected smart spaces are acting as agent for crowd-sensing. An example of this merging is the control and monitoring of smart grid infrastructures via the use of mobile phones powered either using Android or iOS. Developments within the interconnected ecosystem and demand or seamless and wireless smart grid, coupled with the defencelessness of the smart connected home, will unavoidably lead to consequences in the event of a hacking attack, malware infection or Distributed Denial of Service (DDoS), while the assortment of interconnected systems will likely convert a hub for criminal events, privacy breaches, and other cyber attacks, developing in a life-threatening security hallucination for users [2]. None of these devices used within such environments are developed and deployed with the capability or consideration of being shielded from hacking. Meanwhile, most IoT devices are designed to operate autonomously without considering long periods security protection.

The pace at which they have been spreading is growing exponentially: multiple studies suggest that more than 20 billion smart devices will be circulating by 2020 [9]. Such a complex interconnection and exchange of information requires the development of sophisticated technologies that will allow users, organizations, and the devices themselves, to be reliable, secure and efficient: the main purpose of a smart object is to make the life of the user easier [26]. The growing presence of these devices in our households also points to a level of trust that the consumer has in them. This reliance also led to question the quality, the security of the whole infrastructure, while pointing to the issue of privacy: where is personal information stored? Are they secured? Can we make sure that what we want to keep quiet, will remain private? These and additional questions were at the start of the development of the paper that this paper will explore.

Information security is can essentially be considered a societal problem rather than scientific issues. IoT provides avenues for people to generate snowballing volume of data, often lacking users knowledge, permissions and knowing its consequences. Whereby, this information is either administered by the service provider cloud service or other third parties. The development and inter-connectivity of smart devices within a connected ecosystem will be a vulnerability threat to an

 ISBN: 978-1-61208-683-5

individual user or a cumulative community of users. It is only now that society is starting to understand the security implications and costs of privacy, in both its legal and ethical senses [1]. Oberheide and Jahanian [29] have explored when and why it is more difficult to secure mobile devices in comparison to non-mobile equivalents. They derive a set of principles for mobile security.

A major issue that will be addressed is the freedom of information currently being presented on the devices that we use every day. At the present, this information is being shown or heard without any regard to whom that information is related too. The paper will address this issue by attempting to identify insecure apps and devices that not only hide or reveal information while been installed hence providing context-based security solutions, in the other words it will build a system which is privacy aware of its surroundings. Preliminary research found out that the concept of privacy is understood in a different way than the one used in this paper. The literature Xu [25] and Brauchi [6] addresses privacy concerns in a parallel to way to security concern, so privacy of information means that they are not shared outside the household or refers in general to the possible unwanted sharing of personal information as an issue of confidentiality [16]. For the aim of the paper, when talking about privacy, it will indicate the personal users privacy, and his ability to decide whether he wants to share his own information with other users, within the household, or not.

Consequently, we will look at the main cyber security challenges of living in a Smart Home, along with the security and privacy threats that are presented in Smart Home Devices today. The outcome of the research will be used to outline fundamental requirements needed to provide secure and confidential operations in Smart Homes, by providing the user the security rating label for each device used within their ecosystems.

The rest of the paper is structured as follow, in section II we highlight the key state of the art and related work. Section III provides a description of our proposed conceptual framework, with more details on the use of traffic light systems as key to device security nutrition labeling. The proof of concept of the framework is been presented and discussed in section IV, with key findings. Sections V concludes the paper with future research directions in terms of creating a moving target defense for zero trust security in a connected home ecosystem that will further enhance out early results using machine learning.

II. RELATED WORK

A major issue that will be addressed with the paper is the freedom of information currently being presented on the devices that we use every day. At the present, this information is being shown or heard without any regard to whom that information is related too. A number of studies have been conducted in reference to the effectiveness of warning labels on cigarettes and food products [13][15], , etc. Purmehdi [20], has indicated that label effectiveness is contingent on the type of expected behavioral outcome. In response to these problems, Kelley et al [14], proposed a solution for creating an information design that improves the visual presentation and comprehensibility of privacy police viewed online. Their privacy label was inspired by a nutrition label which summarized website privacy policies.

It has been shown that displaying uncertain data visually enables users to understand better. This has been established on food nutrition labels [24]. Supermarkets and food manufacturers have helped users decide between products by using traffic light color-coded labels. Color-coded nutritional information, as shown in Figure 1, gives users at-a-glance information. By the glance, users can quickly see if the food has high (red), medium (orange) or low (green) amounts of fats, saturates, sugars and salt [18].

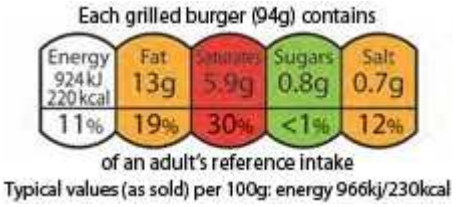

Figure 1. Food Nutrition Label [28]

III. PROPOSED CONCEPTUAL FRAMEWORK

Based upon our research findings, the paper provides a road-map and a visual proposal has been designed for both users and manufacturers which identifies the key issues and vulnerabilities in Smart Devices. This design provides a solution to the key problems of this research which is to extend awareness for both stakeholders. Many users are unaware of what potential threats, vulnerabilities, and issues there are and how many of those Smart Devices contain. By displaying each security component in a red, orange and green color code, users will visually be able to see what risks the device has and whether it is safe to have in their home. Whilst this proposal will be beneficial for users purchasing Smart Devices, it will also help guide manufacturers to make better decisions when designing the product.

Following the food nutritional label, the security nutritional label key and colors are presented in Figure 2. The traffic light color system is well known to users around the world and has been utilized by other industries. Applying the system to our proposal, users can effectively understand what each color represents. In this approach, we are targeting a label system that educates the stakeholder on a safe use of the smart device and the potential risk that such devices can be to other users in the smart ecosystems as a whole.

Information on the label for Smart Devices includes:

- Vulnerability: This will show users an overall estimation of how vulnerable the device is. It will take into consideration the security and privacy aspects and the possible attacks the device is vulnerable to. It will also confirm whether there are default passwords and if so, advising users to change the password straight away
- Operating System (OS): This will state the OS of the device and how vulnerable it is to attacks. It will show if the device updates are automatic or whether users have to update them their selves. A recommended timescale is given to show how often to look.
- Privacy: This will show how much confidential personal data is being collected and used by the manufactures and third-parties

- Threats: This will display the possible threats the device is vulnerable to.

Figure 2. Key and for security food label

This design provides benefits for both users and manufacturers. At first glance, users can automatically see that this device is vulnerable and insecure due to the colors presented. The label informs the users briefly about what threats and privacy issues the device is susceptible to.

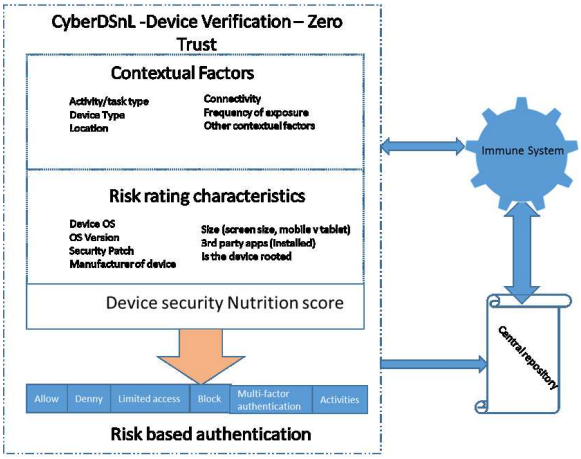

Figure 3. Conceptual Model

Manufacturers will benefit from the use of these labels as it will make them more aware of the designing process. The nutritional label currently seen on food and drink makes users instantly aware as to how sugary it is or how much fat is contained from the colors presented on the label. This type of label on Smart Devices will aid in manufacturer sales whilst boosting user awareness. As manufacturers continuously improve their devices, the awareness will continuously grow until every user is fully aware of the current risks. Convenience will no longer be a priority for an average user. It is important to note that this design is a short-term solution for Smart Devices in homes, as smart technology is continuously evolving over time. Our proposed road-map is based on the conceptual model depicted in Figure 3 which is based on the principles of (VAR) corresponds to VISIBILITY, AWARENESS, and RESPONSE to facilitate a proactive device security nutrition labeling approve. Where we identified some vital contextual factors which have the influence to security risk rating of various devices based on the device features and installed 3rd part applications within the device as well as the context on which the device is been used.

IV. Proof of Concept

As a proof of concept for our proposed road-map and conceptual module, we have developed an Android app that is able to dynamically analysis the contents of the devices that are installed on and is able to inform the user the risk rating or security nutrition label of the device. Where the app is able to dynamically deactivate the access to certain activities within the device and the ecosystem based on the overall security score/rating of the device. To achieve this we have considered the following key context and characteristics:

- Device OS,
- OS version,
- API,
- Security patch last updated,
- Days since the last update,
- Make Model,
- Screen size,
- is the device rooted?

This will then give a device security score. Device score is as follows, and has been worked out using metrics specified below:

- 1 -3 (Green / low-security risk)
- 4-5 (Amber/medium security risk)
- 6-10 (Red / high-security risk)

All devices start out with a score of 1 by default and the score is added to if risks are identified, such as;

- If the device is rooted - score = 6 (automatically high risk)
- If the device hasn't had a security patch in 120 days or more - score = 4
- If the device security patch is over a month old, but not yet 3 months old - score = 3
- If the device OS is out of date (i.e. less than 8) - score = 4
- If the device OS is up to date, but not the latest API (i.e. if it is 8.0, not 8.1) - score = 3

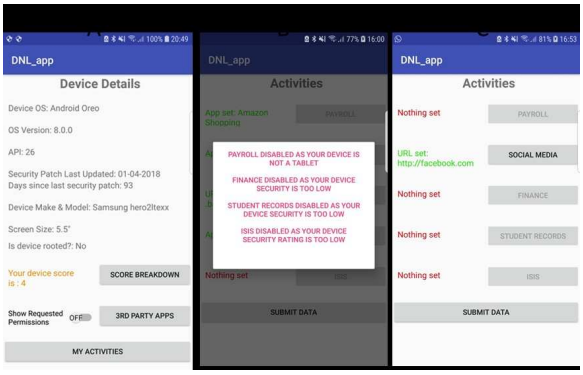

Figure 4. Device Score and a Warning message

The app also looks at the 3rd party apps installed on the phone and their permissions and how many have 40% or more

requested permissions than actual permissions as shown in Figure 5 (B).

- If 4 or more 3rd party apps have - score = 4
- If less than 4 3rd party apps have - score = 3 (still Green)
- If none (which would be impossible I feel) then change to the score (still 1).

The app allows the user to launch other activities, which they set themselves (for proof of concept only) based on the following scores, score breakdown and permitted activities are presented in Figure 5

- Payroll allow only when green and bigger screen size (Tablet, so 6" or greater)
- Social media amber or green
- Finance only green
- Student record only green
- ISIS only green, bigger screen size,
- if OS not up to date, automatically deny even if overall rating is green

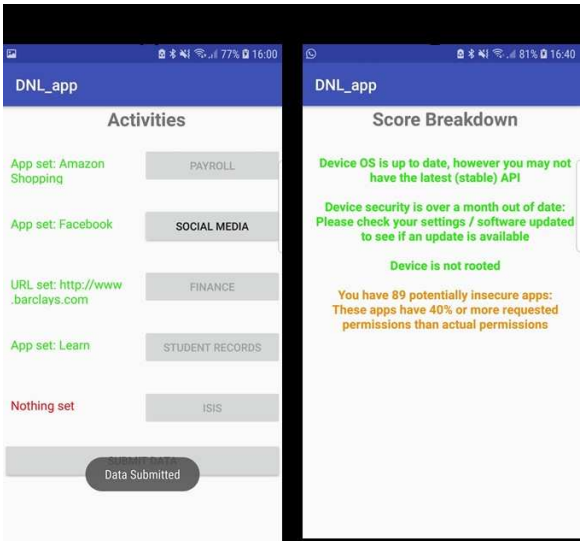

Figure 5. Activity List and Score Breakdown

The end user (admin) can set either a website Figure 4 (C) or app Figure 5 (A) on their phone which is launched when they click the relevant button, assuming the button/activity has not been disabled due to their device score, screen size etc. Lastly, the end user can submit their device data to a Gmail account/form, this submits/lists all the information from the front screen along with how many potentially insecure 3rd party apps are on the device. This data is aim to be used as a training set for the future aspect of this prototype the immune systems depicted in the conceptual model presented in Figure 3.

V. CONCLUSION

IoT is undoubtedly transforming our daily lives by creating opportunities to live better and more efficiently. The increase of Smart Devices is transforming residential homes into Smart Homes. Sooner rather than later, every home will evolve into a Smart Home due to the numerous benefits they provide. However, whilst the benefits of Smart Homes may outweigh the problems for users it is important to address the security-related challenges and concerns within this domain. We have provided a brief description and analysis of the issues of smart device, and the main contribution of our paper is in term of providing a conceptual framework and road-map to a more secure devices security ecosystems based on lessons learned from nutrition labels in both food and tobacco industries. The next step of this paper is to provide a proof of concept that will demonstrate the effectiveness of this framework and road-map to the cyber security ecosystems of smart spaces while highlighting the benefits of the road-map to the three-fold contribution/aims of the paper. This will further be enhanced by providing a proof of concept and more intelligent zero-trust framework for CyberSDnL.

ACKNOWLEDGMENT

The authors appreciate the help and some funding from the CodeWest project, which has supplied some funding for the development of the proof-of-concept presented in this paper. Also, our appreciation goes to the students who helped with the prototype and the background work on the research.

REFERENCES

[1] A.Arabo, I. Brown, F. Musa, "Privacy in the Age of Mobility and Smart Devices in Smart Homes", 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk, and Trust, pp. 803-809, 2014

[2] A. Arabo, "Cyber Security Challenges within the Connected Home Ecosystem Futures." Procedia Computer Science, 61, pp.227-232.

[3] N. Apthorpe, D. Reisman, and N. Feamster, "Closing the Blinds: Four Strategies for Protecting Smart Home Privacy from Network Observers," Cornell University Library. pp. 2. [Accessed 5 October 2018].

[4] N. Apthorpe, D. Reisman, S. Sundaresan, and N. Feamster, "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic", arXiv.org [Accessed 11 October 2018].

[5] M. Barnes, "Alexa, are you listening?. MWR InfoSecurity", Available from: https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening/ [Accessed 26 October 2018].

[6] A. Brauchli, D. Li, " A Solution-Based Analysis of Attack Vectors on Smart Home Systems. In:Fei, Security, and Privacy in the Internet of Things (IoTs): models, algorithms and implementation." Taylor Francis Group. pp. 92-106.

[7] S. Bustamante, P. Castro, A. Laso, M. Manana, A. Arroyo, " Smart Thermostats: An Experimental Facility to Test Their Capabilities and Savings Potential " Sustainability. 9 (8), pp. 1462. [Accessed 7 November 2018].

[8] R. L.Finn, D. Wright, and M. Friedewald, "Seven Types of Privacy. European Data Protection: Coming of Age, Dordrecht", Springer, pp3-32.

[9] Gartner "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016." Available from: https://www.gartner.com/newsroom/id/3598917 [Accessed 4 November 2018].

[10] M. Ghiglieri, M. Volkamer, and K. Renaud, "Exploring Consumers Attitudes of Smart TV Related Privacy Risks [online]". Human Aspects of Information Security, Privacy, and Trust. pp. 656-674. [Accessed 3 October 2018].

[11] W. Haack, M. Severance, M. Wallace, and J. Wohlwend, " Security Analysis of the Amazon Echo [online]". pp. 1-10. [Accessed 7 November 2018].

[12] C. Jackson, & A. Orebaugh, "A study of security and privacy issues associated with the Amazon Echo [online]". International Journal of Internet of Things and Cyber-Assurance. 1 (1), pp. 91-98.

 ISBN: 978-1-61208-683-5

[13] J. Kees, S. J. Burton, C. Andrews, and J. Kozup , ”Tests of Graphic Visuals and Cigarette Package Warning Combinations: Implications for the Framework Convention on Tobacco Control.” Journal of Public Policy Marketing: Fall 2006, Vol. 25, No. 2, pp. 212-223.

[14] P. Kelley, J. Bresee, L. Cranor, and R. Reeder, ” A ”nutrition label” for privacy [online]. Proceedings of the 5th Symposium on Usable Privacy and Security” - SOUPS ’09. [Accessed 21 October 2018].

[15] N. Khandpur, P.M. Sato, L.A. Mais, A.P.B. Martins, C.G. Spinillo, M.T. Garcia, C.F.U. Rojas, P.C. Jaime, ” Are Front-of-Package Warning Labels More Effective at Communicating Nutrition Information than Traffic-Light Labels? A Randomized Controlled Experiment in a Brazilian Sample.” Nutrients 2018, 10, 688

[16] H. Lin, N. W. Bergmann, ” IoT Privacy and Security Challenges for Smart Home Environments.” Information. 7 (44), pp.

[17] R. Miao, R. Potharaju, M. Yu and N. Jain, ”The Dark Menace.” Proceedings of the 2015 ACM Conference on Internet Measurement Conference - IMC ’15. pp. 170. [Accessed 16 October 2018].

[18] NHS ”Food labels. [online]”. Available from: https://www.nhs.uk/Livewell/Goodfood/Pages/food-labelling.aspx [Accessed 20 October 2018].

[19] A. Prasad, ” Exploring the Convergence of Big Data and the Internet of Things.” IGI Global.

[20] M. Purmehdi, R. Legoux, F. Carrillat, and S. Senecal , ”The Effectiveness of Warning Labels for Consumers: A Meta-Analytic Investigation into Their Underlying Process and Contingencies.” Journal of Public Policy Marketing: Spring 2017, Vol. 36, No. 1, pp. 36-53.

[21] SAP National Security Services, Inc ” Cracking the conundrum of IoT convenience and security – what’s next?. [online]”. Available from: https://www.sapns2.com/cracking-conundrum-iot-convenience-security-whats-next/ [Accessed 6 October 2018].

[22] C. Stergiou, K. Psannis, B. Kim, and B. Gupta, ” Secure integration of IoT and Cloud Computing.” Future Generation Computer Systems. 78pp. 964-975.

[23] Trend Micro ”A Look Into the Most Noteworthy Home Network Security Threats of 2017.[online]”. Available from: https://www.trendmicro.com/vinfo/au/security/research-and-analysis/threat-reports/roundup/a-look-into-the-most-noteworthy-Home-network-security-threats-of-2017 [Accessed 1 November 2018].

[24] M. Vasiljevic, R. Pechey, and T. Marteau, ” Making food labels social: The impact of colour of nutritional labels and injunctive norms on perceptions and choice of snack foods.” 91pp. 56-63. [Accessed 20 October 2018].

[25] C. Xu, X. Zheng X. Xiong, ” The Design and Implementation of a Low Cost and High Security Smart Home System Based on Wi-Fi and SSL Technologies.” Journal of Physics: Conference Series 806 012012.

[26] I. Andrea, C. Chrysostomou, ” Internet of Things: Security vulnerabilities and challenges.” Computers and Commmunications (ISCC), 2015 IEEE Symposium on. pp. 180-187.

[27] S. Zheng, M. Chetty , and N. Feamster, ” User Perceptions of Privacy in Smart Homes” [online]. arXiv.org [Accessed 25 Octover 2018].

[28] Food Standards Agency ”Food nutrition label. [online].” Available from: https://www.food.gov.uk/northern-ireland/nutritionni/fop-ni [Accessed 15 October 2018].

[29] J.Oberheide, and F. Jahanian, ”When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments”, Proceedings of the Eleventh Workshop on Mobile Computing Systems Applications, pp.4348.

 ISBN: 978-1-61208-683-5