Pervasive eHealth services a security and privacy risk awareness survey

Bellekens, Xavier
Seeam, Preetila
Franssen, Quentin
Hamilton, Andrew
Nieradzinska, Kamila
Seeam, Amar

Bellekens, X. et al. 2016. Pervasive eHealth services a security and privacy risk awareness survey. International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, 13-14 June 2016.

Pervasive eHealth Services
A Security and Privacy Risk Awareness Survey

Xavier Bellekens
Division of Computing
and Mathematics
Abertay Dundee University
Email: x.bellekens@abertay.ac.uk

Preetila Seeam
School of Management and Business
Aberystwyth University
(Mauritius Branch Campus)
Quartier Militaire, Mauritius

Quentin Franssen
Cyber-Physical Security
Cyber Security Division
IT Risk and Assurance
Financial Service Advisory

Andrew Hamilton
Department of Electronic
and Electrical Engineering
University of Strathclyde
Glasgow, G1 1XW, UK

Kamila Nieradzinska
Department of Electronic
and Electrical Engineering
University of Strathclyde
Glasgow, G1 1XW, UK

Amar Seeam
School of Science and Technology
Middlesex University
(Mauritius Branch Campus)
Vacoas, Mauritius

***Abstract*—The human factor is often recognised as a major aspect of cyber-security research. Risk and situational perception are identified as key factors in the decision making process, often playing a lead role in the adoption of security mechanisms. However, risk awareness and perception have been poorly investigated in the field of eHealth wearables. Whilst end-users often have limited understanding of privacy and security of wearables, assessing the perceived risks and consequences will help shape the usability of future security mechanisms. This paper present a survey of the the risks and situational awareness in eHealth services. An analysis of the lack of security and privacy measures in connected health devices is described with recommendations to circumvent critical situations.**

I. Introduction

Situational and risk awareness are the processes leading to a decision. The results obtained by measuring the awareness of users can provide valuable inputs on the decision making process of a group. In the world of cyber-security, risk awareness plays an essential role in the decision making process of the users and their behaviours when faced with a cyber threat. Convincing the users to comply to defined rules is often difficult and dependant on the knowledge and understanding of the users. This can lead to irrational choices, resulting in the rejection of new security measures due to perceived low benefits [1].

This paper demonstrates the risk awareness of users in the context of connected wearables. The research is survey based, with a total of 273 participants from different backgrounds and from different parts of the world. The data obtained demonstrate a low understanding of the threats faced by connected objects and more particularly by connected wearables. The results gathered by the survey also suggests that a vast majority of users underestimate the risk encountered when using connected wearables and often trust the service and hardware provider to ensure maximum security. This research also provides a method to alleviate the consequences of threats faced by the users as well as means to educate participants on the benefits of security and privacy measures.

II. Online Risk Awareness Survey

The survey was designed and ran as an online questionnaire, allowing the perceived risks and situational awareness of the user in the context of connected wearable health devices to be assessed. A survey was chosen as the research methodology as it allows a wide range of diverse people to be sampled [2]. The survey also gave an initial understanding of the perceived risks independent of the culture or belief which may often influence the risk awareness.

To investigate the awareness of different type of users, the survey was ran on multiple continents, using Amazon's Mechanical Turk,international higher education students located in Mauritius, and requested undisclosed professional participants from large SME's in the technology business.

The survey was designed in a user-centric fashion, assessing the risks participants could be subject to while possessing a wearable health device and uploading data towards a centralised server. Different scenarios were presented to the participants and the user was requested to highlight the risks they were aware of. Furthermore, the participants were requested to categorise the different risks, as well as their general awareness of recent events such as data leaks, Infections (Malwares, Viruses), Compromised websites, etc.

A. Participants

In order to provide accurate results, we selected participants from different backgrounds, such as students from different Universities and we also submitted the survey to a number of professionals working within areas close to or related to information security. We also submitted the questionnaire

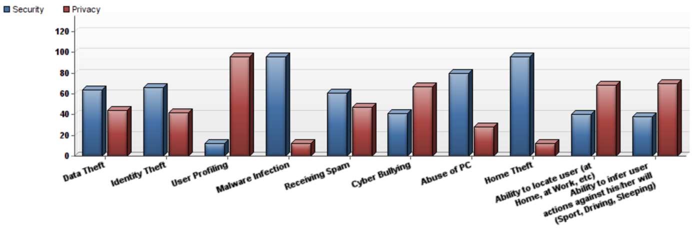

Fig. 1. Risk type awareness answers from different participants

to Amazon Mechanical Turk [3] [4]. MTurk participants were all based in the United States, and were offered $ 2 to complete the survey. The MTurk participants were all Master workers, screened by Amazon for their reliability and on the number of tasks they have previously successfully completed. All results received via MTurk were screened for irregularities and random answers, to prevent abnormalities occurring within the final analysis.

This technique allowed the identification of major differences in the situational awareness of the participants, based on their age, countries and education. Overall we gathered 148 valid answers from MTurk, 110 answers from students, and 15 answers from professionals. An overview of the participants can be found in Table II-A.

	Students	MTurk	Professionnals
Participants	110	148	15
Male	72 %	51%	86.7%
Female	28 %	49%	13.3%
Age Range	17-36	21-69	24-53
IT Experience	76%	59%	100%
Posses Wearables	53%	46%	24%

III. Results

This section highlights the answers gathered from the 273 participants across the different scenarios and analyses the results. The conclusions drawn from the different scenarios and questions apply equally for the students, professionals and the MTurk users unless stated otherwise.

Figure 1 demonstrates the situational awareness of the participants when trying to categorise threats. The results indicate that the majority of participants are aware of the differences between security and privacy. However, Data and Identity theft are often categorised by the participants as a security concern, rather than a privacy concern, highlighting a grey area between privacy and security. This behaviour was similar between all participants.

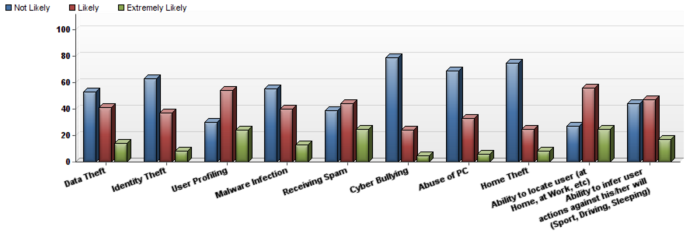

Fig. 2. Evaluation of threat likelihood by participants

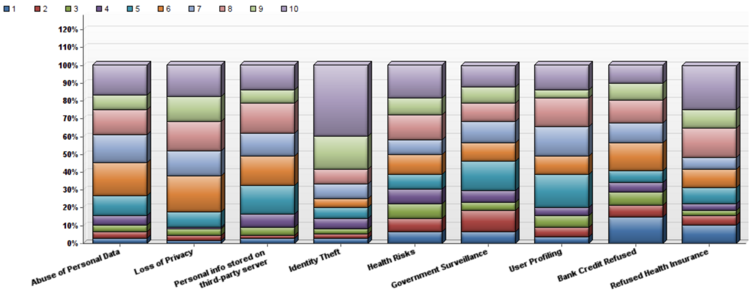

Fig. 3. Evaluation of threat severity

Figure 2 demonstrates the risk awareness of the participants and the relevance of each threat when using a connected wearable device. It is indicated that over 80% of users are not aware of cyber bullying when in possession of wearables. However, as highlighted in [5] most services offer to share the performances of the users on social networks, which could lead to cyber-bullying.

Furthermore, over 70% of the participants were not aware of the risk of home theft when possessing and sharing data on social networks via their connected device as explained in [6]. The information and metadata shared by the users can be used by for criminal purposes such as theft.

The results also indicate that the majority of participants believe that such breaches and threats are unlikely to happen, despite the participants demonstrating concern towards these threats. These results are consistent with previous situational awareness surveys [1].

Figure 3 demonstrates the participants threat severity awareness based on current events [7] [8] and current threats [9] [10]. Grade 1 represents low severity while grade 10 represents the maximum severity. The results indicate that over 45% of the participants view ”identity theft” as highly severe.

Over 35% of participants also demonstrated great concern regarding the data ownership, and the possibilities of their data being shared with insurance companies. A quarter of the MTurk users also believed some personal data were already being transmitted to insurers and believed they could be refused policies based on their lifestyle. Interestingly, all professionals and over 69% of students expressed their concerns regarding personal data shared with third parties but believed that it would be explicitly stated if the data had been shared.

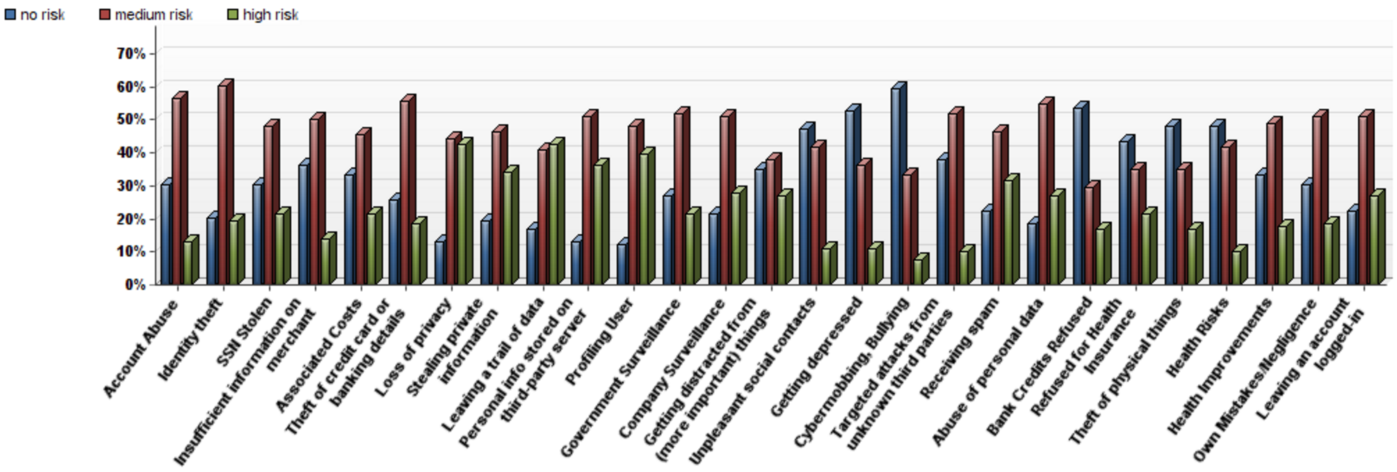

Fig. 4. Based on their personal experience, participants were asked to rate risks of each threat

Moreover, over 89% of the participants currently owning a connected wearable device admitted that they had never read the privacy policies and had never read any amendements made by the company providing the monitoring services despite being notified by email. However, over 92% of all participants stated that they would be more inclined to view a video of the amendments or an informative animation rather than reading amendments.

15.13% of the participants rated mortgage refusal with the lowest severity, despite numerous concerns raised by the press and some early examples of discrimination [11]. The mean rating however, provided a severity score of 5.5, classified as medium severity.

Interestingly *User Profiling, Government Surveillance* and *Personal Information Stored by Third Parties* did not raise much concern with a mean of 4.5, 6.1 and 5.9 respectively.

Figure 4 demonstrates the participants risk awareness based on their personal experience only. The results indicate that over 56% and over 59% of participants classified *Account abuse* and *Identity theft* respectively as a medium risk. The participants however demonstrated less concern to *cyber bullying* and *Mortgage Refusals* with over 55% and 50% respectively. However, over 34% participants rated health insurance refusal as a medium risk.

The highest risks identified by the participants were *Stealing Private Information*, *Loss of Privacy*, *Leaving Trails of Data and Metadata*, and *User Profiling*, with 35%, 44%, 41%, 40% high risk ratings respectively.

Figure 5 assessed the understanding and overall cyber-security awareness of the participants. The participants were asked about recent data breaches covert in major media [12] [13] [14]. It was demonstrated that 65% had never heard of connected wearable hacking, and over 52% of participants had never heard of IoT/connected devices fraud or misuse.

Following these questions 97% of participants believed the personal data provided by connected wearables should be subject to strict regulations and over 85% of participants would be favorable for end-to-end encryption.

IV. Discussion

The results indicate that the vast majority of the participants trust the services they are using with regards to security and privacy. The users also demonstrate limited knowledge and awareness of current threats and consider themselves and the devices to be immune to a large majority of threats. Numerous participants also demonstrate an unclear understanding of risks and threats, further compromising their awareness. The responses suggest that the loss of privacy implicated by the threats are also unclear. Similar results are observed in [15] were Wash et al. explain that users often lack IT knowledge and are likely to underestimate threats.

A. User Awareness

The survey also indicated that self-negligence was not considered by the participants, further demonstrated the lack of

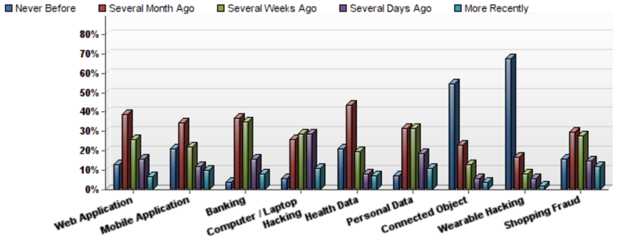

Fig. 5. Assessing the overall Cyber-Security Threat Awareness of Participants

understanding of the different threats. As most of the devices are user-centric, numerous actions such information sessions, risk management information and e-learning can be employed to raise the participants awareness [16] [17] and mitigate the risks.

B. Regulations

When considering user trust in devices and software, a number of regulations should be defined by the European Union and other legislative bodies to provide a legal framework and uphold data privacy and confidentiality. A number of frameworks for cyber-critical infrastructures have been proposed in the past [18] however, these regulations do not cover the legal aspects, but rather a mean for the service provider to ensure security of the devices.

V. Conclusion

This work introduced risk awareness of pervasive connected wearables and demonstrated that the sampled users often perceived a lower risk for themselves or their wearables compared to actual threat level users may face. The participants demonstrated poor understanding of threat protections and often demonstrated a lack of understanding of the particular technologies they are using. Further, participants were not aware of the consequences that threats may have on them personally. This research also highlights the lack of engagement users are willing to provide to understand the security and privacy policies related to the devices they are using. The work also indicates that users are resilient to new security measures and highlight a number of factors that could lead to the adoption of new security measures in the field of connected wearable technologies. New security and privacy measures should be designed with a focus on the end-user and should be advertised to the user as a benefit that ultimately improves their risk awareness whilst improving the overall threat understanding. Future work should focus on analysing the security and privacy of individuals in the fields of connected eHealth devices. The results presented by this survey lay the foundations for future risk awareness for pervasive eHealth service.

References

[1] M. Evangelopoulou and C. Johnson, “Attack visualisation for cyber-security situation awareness,” in *System Safety and Cyber Security (2014), 9th IET International Conference on*, pp. 1–6, Oct 2014.

[2] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum, “Users’ conceptions of web security: A comparative study,” in *CHI ’02 Extended Abstracts on Human Factors in Computing Systems*, CHI EA ’02, (New York, NY, USA), pp. 746–747, ACM, 2002.

[3] G. Paolacci, J. Chandler, and P. G. Ipeirotis, “Running experiments on amazon mechanical turk,” *Judgment and Decision making*, vol. 5, no. 5, pp. 411–419, 2010.

[4] M. Buhrmester, T. Kwang, and S. D. Gosling, “Amazon’s mechanical turk a new source of inexpensive, yet high-quality, data?,” *Perspectives on psychological science*, vol. 6, no. 1, pp. 3–5, 2011.

[5] M. Kinnunen, S. Q. Mian, H. Oinas-Kukkonen, J. Riekki, M. Jutila, M. Ervasti, P. Ahokangas, and E. Alasaarela, “Wearable and mobile sensors connected to social media in human well-being applications,” *Telemat. Inf.*, vol. 33, pp. 92–101, Feb. 2016.

[6] S. Mann, “Wearable computing as means for personal empowerment,” in *Proc. 3rd Int. Conf. on Wearable Computing (ICWC)*, pp. 51–59, 1998.

[7] “Nsa files decoded:what the revelations mean for you..” http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Accessed: 2016-02-22.

[8] J. B. Rule, D. McAdam, L. Stearns, and D. Uglow, “Documentary identification and mass surveillance in the united states,” *Social Problems*, vol. 31, no. 2, pp. 222–234, 1983.

[9] D. Kotz, “A threat taxonomy for mhealth privacy.,” in *COMSNETS*, pp. 1–6, 2011.

[10] M. Plachkinova, S. Andres, and S. Chatterjee, “A taxonomy of mhealth apps – security and privacy concerns,” in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, pp. 3187–3196, Jan 2015.

[11] “The chart that proves mortgage lenders are ageist.” http://www.telegraph.co.uk/finance/personalfinance/borrowing/mortgages/11750998/The-chart-that-proves-mortgage-lenders-are-ageist.html. Accessed: 2016-02-22.

[12] “What does fitbit hacking mean for wearables and iot?.” http://www.welivesecurity.com/2016/01/12/fitbit-hacking-mean-wearables-iot/. Accessed: 2016-02-22.

[13] “Biggest hacking threat to business? wearables.” http://www.cnbc.com/2015/03/17/biggest-hacking-threat-to-business-wearables.html. Accessed: 2016-02-22.

[14] A. Wright, “Hacking cars,” *Communications of the ACM*, vol. 54, no. 11, pp. 18–19, 2011.

[15] R. Wash, “Folk models of home computer security,” in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS ’10, (New York, NY, USA), pp. 11:1–11:16, ACM, 2010.

[16] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness,” *MIS Q.*, vol. 34, pp. 523–548, Sept. 2010.

[17] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, “A video game for cyber security training and awareness,” *computers & security*, vol. 26, no. 1, pp. 63–72, 2007.

[18] X. Bellekens, A. Seeam, K. Nieradzinska, C. Tachtatzis, A. Cleary, R. Atkinson, and A. Ivan, “Cyber-physical-security model for safety-critical iot infrastructures,” in *Wireless World Research Forum Meeting 35*, no. WWRF35, 2015.