OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

RELINK PROJECT

Title: Annotated_Bibliography_EPS_Group_5

Type: Annotated Bibliography

Description

This document describes the; Annotated_Bibliography_EPS_Group_5

Course:	EPS
Document version:	1.0
Status:	Release
Author:	EPS Group 5
Date:	11-Apr-2024

1 User Perceptions of Smart Home IoT Privacy

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 200:1-200:20. https://doi.org/10.1145/3274469

Summary

This study consisted of interviews with smart home device owners to investigate the purchasing decision process, user perceptions of the privacy risks and actions taken to protect themselves. The study results highlight that users prioritize convenience over anxieties surrounding data privacy and security. Users are willing to accept these potential risks even if they are aware of the trade-off. Additionally, they are unaware of privacy risks from devices that do not record audio or video.

Relevance

This article is useful as it studies user perceptions on privacy questions raised by smart home devices, which is the focus of our study. It also shows how users are unaware of certain threats. For example, users believe that devices that don't record audio or video don't pose privacy risk because the collected data is not sensitive. We are using this to write a chapter on our educative website.

2 "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products

Chalhoub, G., Kraemer, M. J., Nthala, N., & Flechais, I. (2021). "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–16. https://doi.org/10.1145/3411764.3445691

Summary

This article reports on a study carried with six households from the UK. Households' members were tasked with selecting their smart home devices to then integrating them in their home. Findings indicated user concerns about intrusiveness and tracking, with the study emphasizing the importance of effective privacy controls and the need for clear consent management. Additionally, examples of technology repurposing were highlighted which shows the importance of designers understanding potential misuse.

Relevance

This paper is relevant to our project as it focuses on families, their user experience and privacy concerns regarding smart home device. Families constitute a primary audience for our website which we want as an educative course on privacy risks of smart home devices. It also includes a useful explanation of how parents often repurpose smart home device for parenting, which is a risk we plan to help navigate with our website.

3 I Want It Anyway: Consumer Perceptions of Smart Home Devices

Wang, X., McGill, T. J., & Klobas, J. E. (2020). I Want It Anyway: Consumer Perceptions of Smart Home Devices. *Journal of Computer Information Systems*, *60*(5), 437–447. https://doi.org/10.1080/08874417.2018.1528486

Summary

This paper highlights the behaviour of consumers regarding SHD's. As the introduction describes: The results show that individuals tend to ignore the potential risks and focus more on potential benefits resulting from using smart home devices. Performance expectancy and compatibility were found to be positively related to perceived benefits. However, neither effort expectancy nor image were. Among the proposed dimensions of risk, only privacy risk, performance risk, and time risk significantly influenced perceived risk. Security risk and financial risk did not influence it.

Relevance

The consumer behaviour is important to highlight in this project, as we want to empower them to get more in control of their SHD. To do this, we need to know what is important for the consumer (i.e the consumer is less concerned about the security of the device and is more concerned about its privacy).

4 Hardware Security in IoT era: the Role of Measurements and Instrumentation

Tudosa, I., Picariello, F., Balestrieri, E., De Vito, L., & Lamonaca, F. (2019). Hardware Security in IoT era: The Role of Measurements and Instrumentation. *2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT)*, 285–290. https://doi.org/10.1109/METROI4.2019.8792895

Summary

The authors stress the importance of hardware security in IoT, highlighting the vulnerability of devices to physical attacks and the potential for malicious circuit injection in custom ICs. They challenge public perceptions of IoT security and outline various attack methods. Furthermore, they identify size, computational capabilities, and power limitations as challenges for small IoT devices, suggesting that the industry's lack of focus on hardware security exacerbates these threats.

Relevance

This paper shows different risks and problems that are happening inside IoT devices. This is useful because it can be used for documentation. While the paper is really technical, the information can be used and parts can be extracted and rewritten in understandable sentences.

5 Transparency in the consumer Internet of Things

Hudig, A. I., Norval, C., & Singh, J. (2023). Data rights in the consumer Internet of Things. *International Conference on AI and the Digital Economy (CADE 2023)*, 25–30. https://doi.org/10.1049/icp.2023.2560

Summary

The paper details research about 43 products in 11 categories of smart home devices. A lot of time was spent contacting vendors to see if they were compliant with UK GDPR, and all of the steps taken & the findings are documented in great detail.

Furthermore, the data flows in all of the devices in question were researched. This includes the number of IPs contacted, the volume of transmitted data, which organizations & countries the IPs belonged to, etc... All of this information is sorted per category of devices and gives insight into what categories are the worst with regards to users' privacy.

Relevance

This paper contains a lot of very detailed research results about both the legal side of data collection and observed data flows in a wide range of IoT devices. I think we can learn a lot from this paper and it is very relevant to our project.

6 Privacy Norms for Smart Home Personal Assistants

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021). Privacy Norms for Smart Home Personal Assistants. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3411764.3445122

Summary

The researchers conducted an online survey to understand users' security & privacy preferences regarding data flows in smart home devices. The result is a chart that shows how comfortable people are with other parties seeing their data (friends, families, lovers, strangers, etc.). Most people are for example comfortable with their partner seeing / having access to their data flows, but not their neighbours or general visitors. A chart is also created for non-user recipients (computer systems). They also list a host of other research papers under section 2.2.

Relevance

This paper is very relevant for us, as it gives a clear insight into users' acceptance with other people / parties viewing / accessing their data.

7 On Privacy and Security Challenges in Smart Connected Homes

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On Privacy and Security Challenges in Smart Connected Homes. *2016 European Intelligence and Security Informatics Conference (EISIC)*, 172–175. https://doi.org/10.1109/EISIC.2016.044

Summary

This paper presents an overview of privacy and security challenges in smart connected homes. It is said that increasing deployment of smart connected devices expose the resident's security and privacy risks as personal information becomes accessible in new ways via remotely. There can be new ways that attacker can eavesdrop on or detect activities such as going to shower. In addition, take over control of the entire home devices.

For example, challenges can be device issues (resource constraints, headless nature or tamper resistant packages), communication issues (heterogeneous protocols or dynamic characteristics) or service issues (longevity expectations). There is mentioned few technological approaches to mitigate security and privacy threats (device, communication and service level).

Relevance

It is related to our topic because these challenges are important to list that people having these devices in their home are informed and understand risks and challenges when using them.