Home Digital Voice Assistants: use cases and vulnerabilities

Oleksandra Baga
Master Computer Science, Freie Universität Berlin
Sommersemester 2021, Seminar Technische Informatik
oleksandra.baga@gmail.com

***Abstract*— Smart speakers with voice assistants achieved last years impressive results in speech recognition enabling more seamless interactions between user and a machine but also raise privacy concerns due to their continuously listening microphones. A better understanding of these aspects can help future smart speaker users to make a right decision about the digitalisation of their homes. For these purposes this paper contains as well a result of research about the functionality of digital voice assistance and the real use cases how people are tending to use a device as the research of actual security and privacy concerns including attack surfaces and vulnerabilities.**

I. INTRODUCTION

The development of the Deep Learning algorithms and Internet of Things last years is opening up a new era in the use of the digital tools that surround us. A combination of various algorithms in Machine Learning, Deep Learning, speech synthesis, and Natural Language Processing (NLP) to providing services to the users makes it possible to achieve impressive results in speech recognition enabling more seamless interactions between user and a machine. It is realistic now to say that in the coming years digital voice assistances probably will come into the use of every household. They could become embedded in users' day-to-day routines, particularly people in a dependent situation, whether elderly or disabled.

However, these undeniable advances should not obscure the questions that voice assistants raise from a data protection perspective, in particular from the point of view of transparency in the way their system functions [**?**]. In the survey by Lau et al. [**?**] smart speaker users and non-users were interviewed to find out their arguments for and against adopting this new technology and their privacy perceptions and concerns. Many non-users believe that these devices are not useful at all and companies are not to be trusted. On the other hand, smart speaker users have fewer privacy concerns and rely on companies to safeguard their personal data which think are not interesting to others [**?**]. The goal of this research is reality check of privacy concerns and myths circulating about voice assistants and the abilities that they are assumed to have. This paper presents the closer look at digital voice assistance functions for a clearer understanding of the logic behind these systems and the security questions they raise for their users.

II. ABOUT

A. What is about?

TODO
Lorem Ipsum

B. Something

TODO
Sapana navaga

III. CONCLUSIONS

TADAM!
THE END

REFERENCES

[1] Nan Z., Xianghang M., Xuan F. Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. `https://wiki.aalto.fi/download/attachments/116657996/IoT-attestation.pdf`. date accessed: 29.04.2021