Home Digital Voice Assistants: use cases and vulnerabilities

Oleksandra Baga
Master Computer Science
FU Berlin, SS2021

MOTIVATION

PEOPLE WITHOUT SMART SPEAKERS

Only **4%** of them would be willing to buy one.
The reasons are:
- "pointlessness" (**67%**)
- security of personal data (**59%**).

OWNERS OF A VOICE ASSISTANT

Have fewer privacy concerns and rely on companies to safeguard their personal data.
53% see it as “real innovation" that will "revolutionise everyday life" .

How does a voice assistant work?

Use technologies like voice recognition, speech synthesis, and Natural Language Processing (NLP) to provide services to the users.

Rely on a cloud-based architecture, since data has to be sent back and forth to centralized data centers.

Is constantly listening. Does not store the audio data and does not perform any operations until a specific wake word has been heard.

Voice assistants have interesting capabilities such as:

* Answer to questions asked by users.
* Play music from streaming music services.
* Set timers or alarms.
* Play games.

* Make calls or send messages.
* Make purchases.
* Provide information about the weather.
* Control other smart devices

Report Structure

00 INTRODUCTION
METHODOLOGY

01 ABOUT DIGITAL VOICE ASSISTANCE

1.1 What is Voice Assistance
1.2 How does Voice Assistance work?
1.3 Third party features

02 USE CASES: HOW PEOPLE REALLY USE VOICE ASSISTANCE

2.1 Entertainment, music and media
2.2 Timers and alarms
2.3 Search and source of information
2.4 Smart Home
2.5 Usage by children
2.6. TBA

03 DIGITAL VOICE ASSISTANTS: ATTACK SURFACE & VULNERABILITIES

3.1 Security and Privacy Concerns
3.2 Accidental Recordings
3.3 TBA

04 VOICE-BASED REMOTE ATTACKS

4.1 Voice squatting attack
4.2 Voice Masquerading Attack

05 CONCLUSION
REFERENCES

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.

[2] Terzopoulos G., Satratzemi M..
Voice Assistants and Smart Speakers in Everyday Life and in Education

[3] Druga, S., Williams, R., Breazeal, C., Resnick, M. Hey Google is it OK if I eat you?: Initial explorations in child-agent interaction.

[4] Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., Wagner, D.
Privacy Attitudes of Smart Speaker Users.

[5] Lau, J., Zimmerman, B., Schaub, F.
Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers.

[6] Lau, J., Zimmerman, B., Schaub, F.
Alexa, Stop Recording: Mismatches between Smart Speaker Privacy Controls and User Needs.

References which survey is planned to be based.
References which are planned to cover in more depth.
References for additional information / width research

REFERENCES

[7] Ammari T., Kaye J., Tsai J.T., Bentley F.
Music, search and IoT: How people (really) use voice assistants.

[8] Amazon.com.
Alexa features.

[9] Commission Nationale de l'Informatique et des Liberts. White Paper Collection.
Exploring the ethical, technical and legal issues of voice assistants.

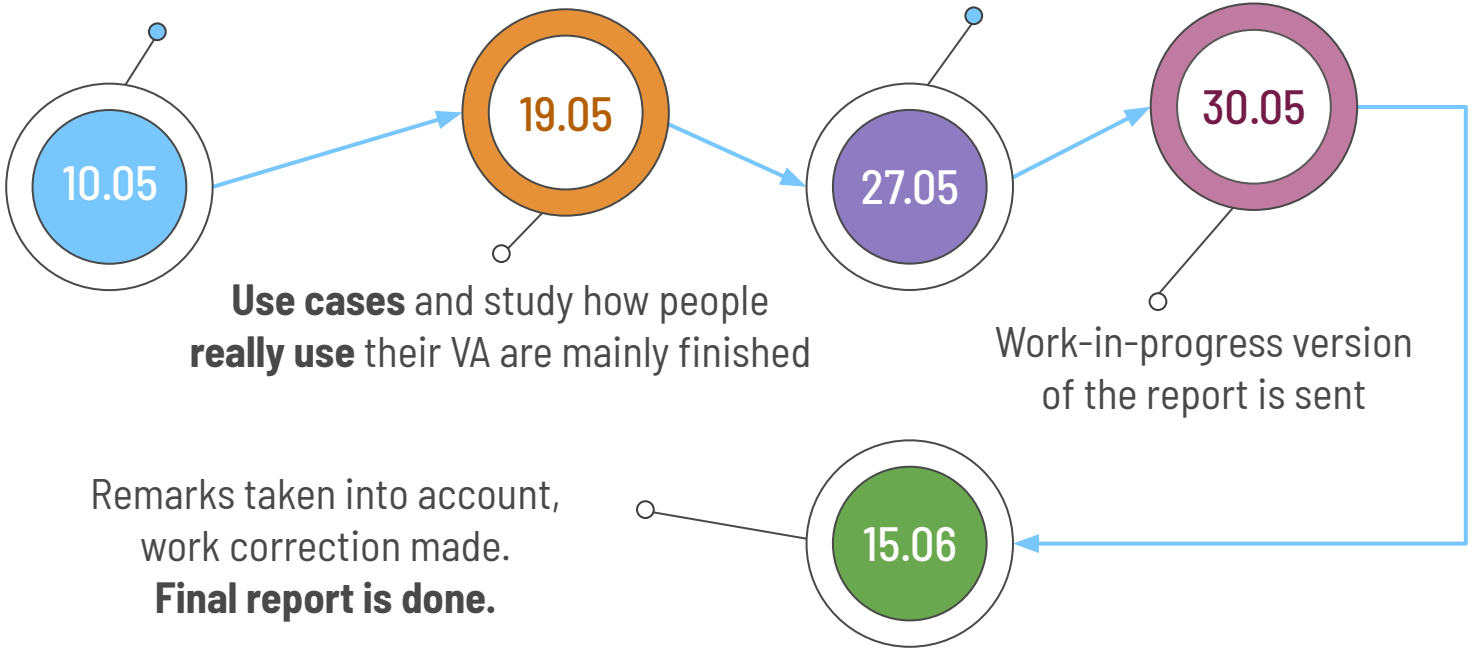
[10] Lei X., Tu L.,Liu A.X., Chi-Yu Li.
The Insecurity of Home Digital Voice Assistants: Vulnerabilities, Attacks and Countermeasures.

[11] Ren J., Dubois D. J., Choffnes D., Mandalar A. M.
Information Exposure From Consumer IoT Devices.

[12] Knote R., Janson A., Eigenbrod L., SIlner M..
The What and How of Smart Personal Assistants: Principles and Application Domains for IS Research.

References which survey is planned to be based.
References which are planned to cover in more depth.
References for additional information / width research

SCHEDULE SPRING–SUMMER 2021



Thank you for your attention!

Oleksandra Baga
Master Computer Science
FU Berlin, SS2021

Do you have any questions?

oleksandra.baga@gmail.com
www.oleksa.de