BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2024

Resilience of Biometric Authentication of Voice Assistants against Deepfakes

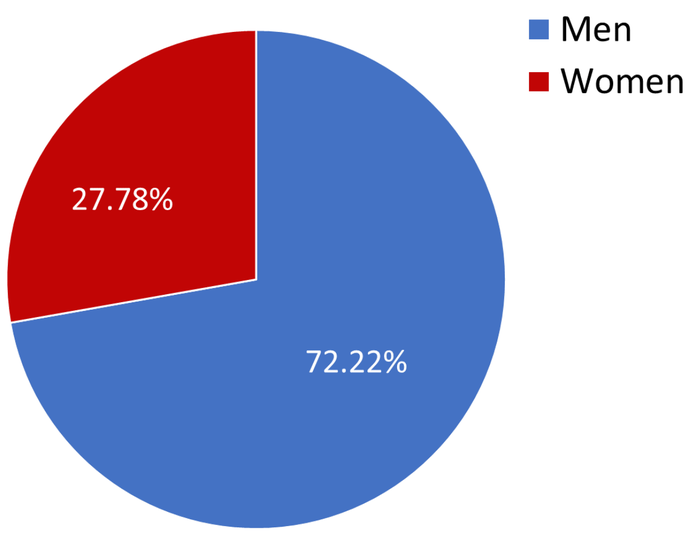
Author: Petr Kaška

supervisor: Mgr. Kamil Malinka, Ph.D.

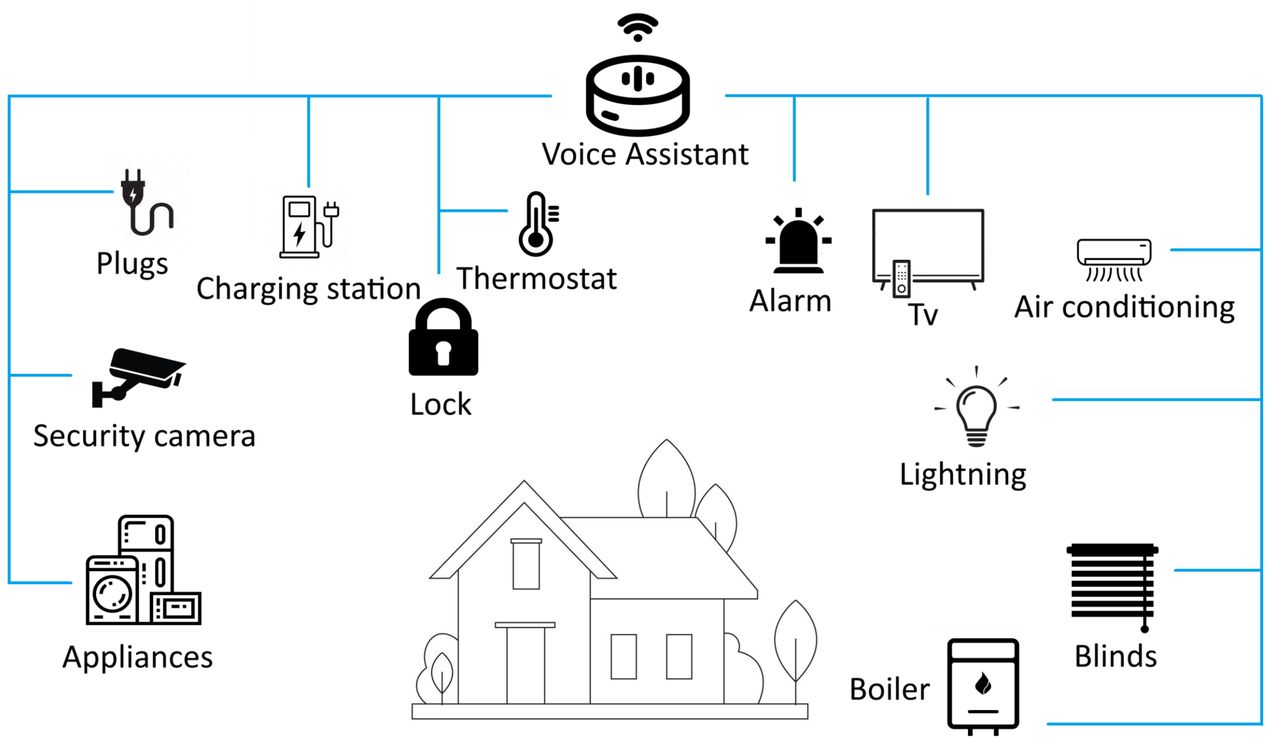
Goal:

- experimentally demonstrate the vulnerability of voice assistants

Gender representation among the 72 participants in the experiment.



Devices and sensors in smart home (possible targets of an attacker)



Metrics used in the evaluation

$$success\ rate\ (\%) = \left(\frac{\text{number of successful trials}}{30}\right) * 100$$

Command analysis -> obtaining knowledge from the pre-expression

Alexa, Ask Daily Horoscopes about Taurus.

Wake word | Phrase | Invocation Phrase | Utterance

Final results