Risk Analysis of Inference Attacks on IoT Wearables

Sebastian Pape, Vanessa Bracamonte, Jacob Kröger, Welderufael Tesfay, Toru Nakamura, Majid Hatamian, Shinsaku Kiyomoto, Kai Rannenberg

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

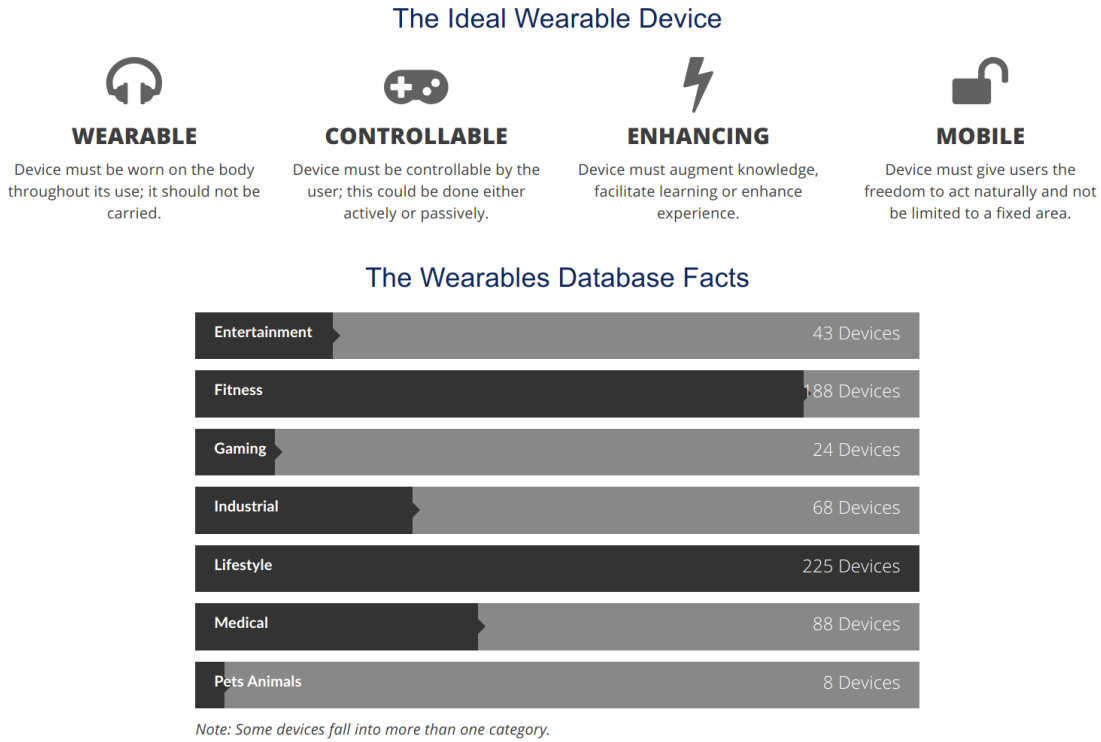
Privacy Enhancing Technologies SIG
German Informatics Society (GI)

November 4th 2020 European Big Data Value Forum Berlin

Agenda

- IoT Wearables
- Inference attacks
  - Example
  - Principle
- Survey on inference attacks
- Framework for risk analysis
- Conclusion

IoT Wearables



[Source: vandrico.com]

IoT Wearables: Sensors

Sensors in IoT Wearables

- Accelerometer
- Camera
- Gyroscope
- Light
- Magnetic field
- Microphone
- RGB(W) sensor
- Power consumption
- Touchscreen

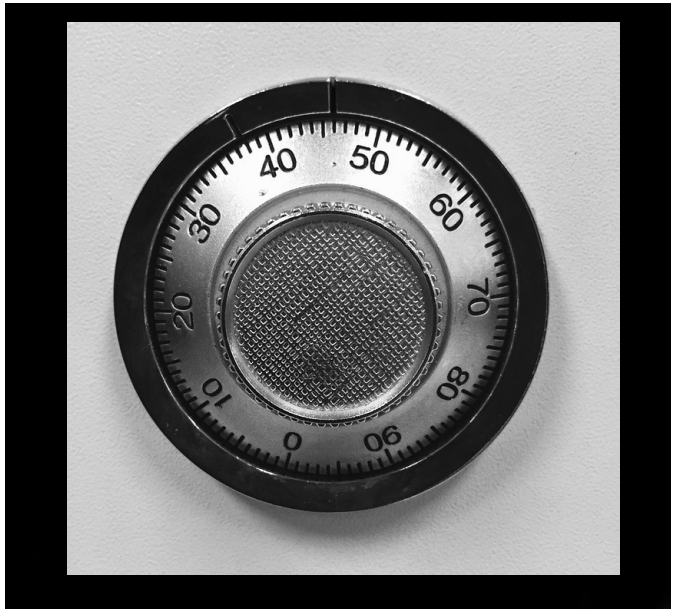
- Glucometer
- Heart Rate Monitor

- Compass
- GPS

- Speaker
- Vibration

Inference Attacks: Example

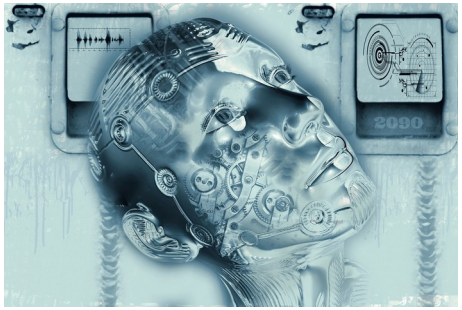
Fitness Tracker



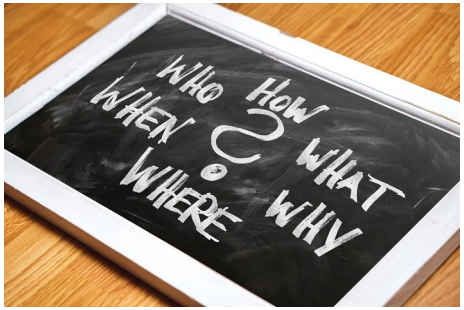
Safe with rotary combination lock

Inference Attacks: Principle

Sensors in IoT Wearables



Machine Learning



Information

Identified Areas

Device Identification

User Input

Localization

Health Data

Demographics

Daily Activities

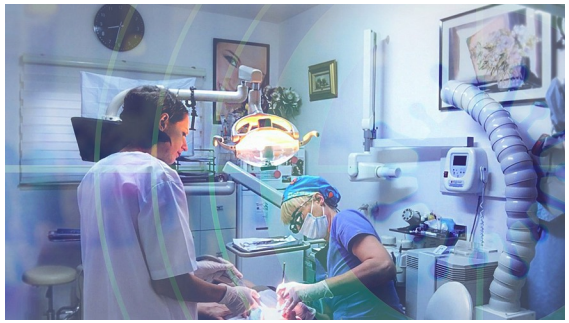
Misc

Conclusion

- 143 inference attacks on IoT Wearables found
  - Many of them surprising
  - Some with harmful impact and quite acurate

- User should be informed before granting access to a sensor
- We should carefully watch what happens with our data

- Problem will be more serious for the Internet of Bodies



Chair of Mobile Business & Multilateral Security

Dr. Sebastian Pape
Goethe University Frankfurt
E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de