- Passwords are Obsolete -
User Authentication through Wearables and Mobile Devices

Background

With the development of smart bands and smart watches by Jawbone, Fitbit, Apple etc., Wearables become ubiquitous. These smart devices not only offer important information at a glance, but also track the user itself and collect various kind of metrics like heart rate or skin temperature used to offer customized fitness apps for running and cycling. Nevertheless, the future usages of such devices and their data are versatile and yet to be researched.

The average internet user (25-34-years-old) has 40 different online accounts. So, in the best case 40 different passwords to remember. Even if we are able to remember each of those passwords, hackers continue to attack services and leak large sets of our passwords. Although those leaks are publicly announced, most user will actually not change their passwords or reuse an old one. It turns out that passwords are outdated.

Description

This bachelor project's goal is to get rid of username/password and create a new user-friendly, easy-to-use authentication mechanism based on life trackers and mobile devices. The idea is to create reliable and secure mechanisms to authenticate a user using his devices by its personal or biometric data.

The bachelor project will focus on multiple subtasks to come up with new authentication schemes:

- Collecting and evaluating data sources for identification
  - Wearables ex. Apple Health, Jawbone[2], Fitbit[4], nymi[5], …
  - Mobile devices ex. Microsoft Band, Pebble, Apple Watch[3], …
  - Smart Phones
  - Hardware tokens (FIDO token)

- Evaluating uniqueness and usability of data
  - How personal is the data?
  - Can we use it for authentication? Is it precise enough?
  - Can we use single features or are combinations more reliable?

- Identification of dependencies between authentication features

- Create Lock-Out criteria to avoid malicious logins

- Keep data security and privacy in mind
  - Bio data should not leave the device
- Development of an authentication prototype
  - Setting up register and login methods
  - Develop algorithms to compare biometric fingerprints

The used programming languages highly depend on the data provider APIs and on the bachelor team itself. Nevertheless, the authentication process should be wrapped into an easy-to-use web interface/service/mobile app using modern frameworks like Angular or React. The final goal is to deploy a prototypically standard compatible service (ex. using OAuth[1]).

Contact

Fachgebiet: Internet-Technologien und -Systeme

- Fachgebietsleiter: Prof. Dr. Christoph Meinel
- Ansprechpartner: Christian Tietz, Patrick Hennig, Philipp Berger
- Projektpartner: Bundesdruckerei

References

[1] http://oauth.net/

[2] https://jawbone.com/up/developer

[3] https://developer.apple.com/watchos/pre-release/

[4] https://wiki.fitbit.com/display/API/Fitbit+API

[5] https://www.nymi.com/