

Master Thesis Behavioral Authentication

“One system to run them all”

Background

Passwords are used for securing computer systems for a long time. Although they are still many times the only protection, people (re-)use short and weak passwords for their own accounts that can easily be guessed or may be revealed by big identity leaks. Apart from possession-based mechanisms like hardware tokens or access cards, behavioral biometrics are usable to verify claimed identities of persons, too and could provide a higher security and usability. Typical examples are the verification by the way a person walks (gait), by the way a person types on a keyboard or touchscreen (keystroke/touchstroke) or by routines based on the browsed webpages, app interaction, or visited locations.

Problem

The core components of any behavioral authentication system are the biometric systems that (pre-)process the sampled human behaviors to apply matching and decision technologies, and possibly fuse these decisions to a final verification or identification decision, e.g., if a system uses gait and keystroke behavior. The established architecture of a biometric system lead to a diverse set of implementation framework proposals for behavioral authentication systems that enable the deployment on Android. In this context, any user of the framework can concentrate on the applied technologies for processing or matching and does not need to care for the typical boilerplate code of pipelines, sensor access, operation system integration, or communication between multiple used devices (e.g., smartphone and notebook). Although there exists many different ideas, a unified framework integrating these proposals is needed, but yet missing.

Goal

In this master thesis, you should develop and evaluate such a unified framework:

- Extensive related work analysis of behavioral authentication frameworks and a classification of them
- Develop a unified behavioral authentication implementation framework architecture and domain model
- Implement the framework that allows an easy integration of new approaches and an easy selection of existing ones for real-world evaluations, for instance.
- Evaluation of the framework by integrating behavioral authentication systems from related work

Contact

Eric Klieme
eric.klieme@hpi.de
H1.18
0331 5509-559