Smartphone Security based on Biometric User Authentication

STU FIIT

Author: Ing. Stanislav Vnenčák | svnencak@gmail.com

Supervisor: Assoc. Prof. Daniela Chudá | daniela.chuda@stuba.sk

MOTIVATION

The way we use mobile devices has changed dramatically in the past few years. Enhanced mobile security is growing in both popularity and importance as our personal and professional lives are managed by data stored in our smartphones.

As there are significant differences in many physiological and behavioral aspects of human beings, behavioral biometrics can introduce a major improvement in mobile security.

METHOD PROPOSAL

Building a biometric user model under a smartphone platform:

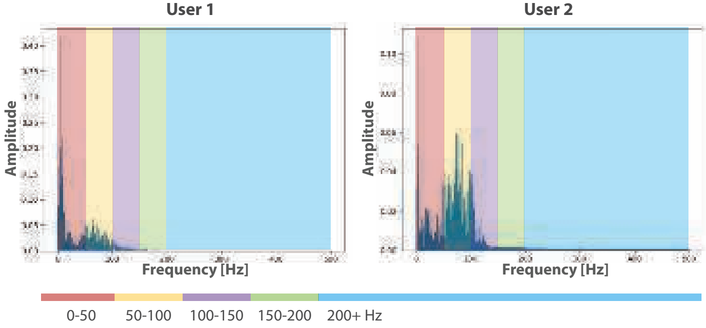
- combination of traditional security methods can provide enhanced and **implicit biometric user authentication method**;
- monitoring user biometric characteristics while working with a mobile device via touch screen or positioning sensors (accelerometer and gyroscope) while unlocking the device with pattern-lock;
- combination of **unlock context identification** and **user verification** (Fig. 1) against context-specific user model;
- user model divided into **pattern-dependent** (PD) and **independent** (PI) **features** with score-level fusion;
- multilayer feature elimination for model minimization.

BIOMETRIC USER MODEL

Result of user characteristics extraction process:

- **91 types** of pattern dependent and independent **user characteristics** (e.g. starting unlock velocity, minor pattern curves diameter or power of dominant accelerometer frequency);
- spectral analysis of accelerometer and rotation data (Fourier transformation) for enhanced biometric model characteristics (Fig. 2);
- specific "**first touch**" characteristics - 24 types (Fig. 3).

Fig. 2 Spectral analysis of accelerometric data with defined frequency bands



DATASET

- **52 participants** for context and user classification;
- 15 100+ unlocks (4 unlock patterns, 2 unlock contexts);
- **long term experiment in unmanaged environment**.

Fig. 1 Process of user authentication (identification + verification)

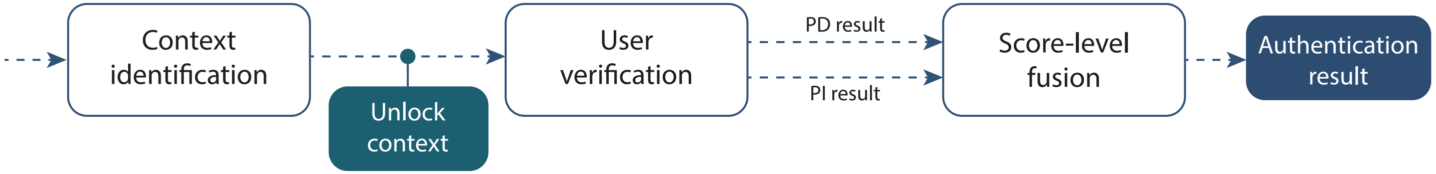
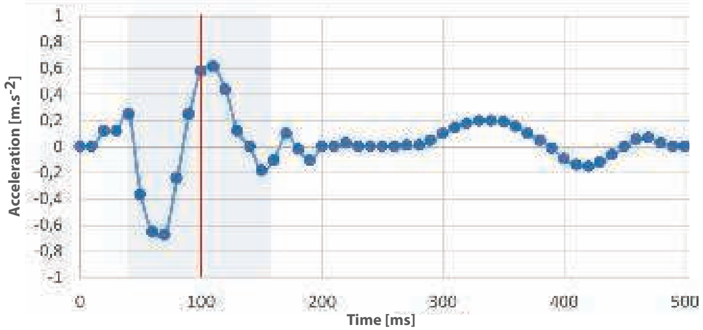


Fig. 3 Accelerometer data with first touch demarcation



EVALUATION METHOD

- high precision in evaluating unlocking context (88%);
- performed **One-Class SVM classification** (Sigmoid kernel) with Cross-validation for biometric system accuracy evaluation;
- minimal error **EER 5.7%** (FAR 21.82%, FRR 28.90%) outperforms existing methods (approx. only 5.7% of all authentications are evaluated incorrectly);
- average improvement in EER 0.48%, FAR 0.05%, FRR 0.23% with proposed feature elimination method with up to 75% model reduction.

CONCLUSION

Proposed method was tested in real environment and authentication accuracy is sufficient for real world applications in respect to:

- proposed **real-time** biometric user authentication;
- no need to store a large volume of users' data with proposed One-Class classification method to prevent security issues and ensure high system efficiency;
- evaluation on unmanaged experiments data;
- reusability in multiple unlock contexts with high authentication accuracy (2-step authentication process).

Slovak University of Technology in Bratislava, Faculty of Informatics and Information Technologies, 2019 STU FIIT