Behavioral Authentication System

Jan Pešek
pesekja9@fit.cvut.cz

Supervisor: prof. Ing. Pavel Tvrdík, CSc.
Department of Computer Systems, FIT CTU in Prague

The Problem

Many smartphone users take their smartphone as a part of everyday life. They use it to manage sensitive content, such as accessing their bank account, which brings additional **security concerns**. Before accessing a session of a secured application a user must prove that he is who he claims to be through an authentication process, which typically consists of **just typing a PIN**. When an attacker can pass that single point of authentication, he can get **access to the account**.

Requirements

The goal is therefore to find an **authentication system that works continuously even after passing that single point of authentication**. However, it is undesirable to ask for additional user interaction. In the context of the number of legitimate accesses to an application, any attack is a rare event. **An intrusive authentication system would ruin the user experience**.

The Solution

Each user has a characteristic behavior when using a smartphone, which is hard to mimic. For example, the way how a user holds the phone, clicks, scrolls, or performs the micro-movements captured by motion sensors. Behavioral authentication continuously evaluates **data produced by sensors or the touchscreen of a smartphone** during an interaction of a user and matches it to the past behavior of the user. This continuous and online processing estimates an authentication score interpretable as a **probability that a session of an application is performed by an attacker**.

System Properties

Use case independent:The owner of the secured application sets the authentication score threshold. The proposed behavioral authentication system provides information without making acceptance or rejection decisions.

Simple maintenance and upgrade: The system is not deployed on a smartphone, instead it is implemented as a centralized web service.

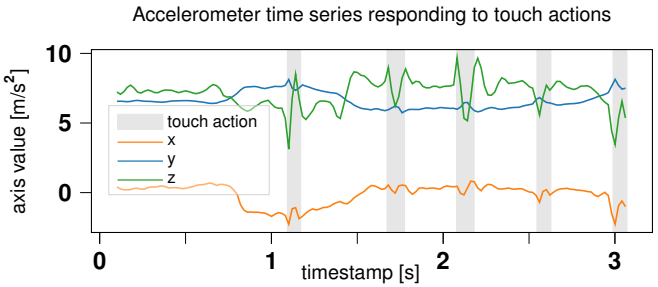
Simulation Environment

This diploma thesis is not supported by any bank and there is not any relevant publicly available dataset for analysis. Therefore, the behavioral authentication system is developed only in a simulation environment. A mobile banking application is simulated using a **custom Android application, called BehavioralCollector**, which consists of 4 activity types:

Login Scrolling Typing Clicking

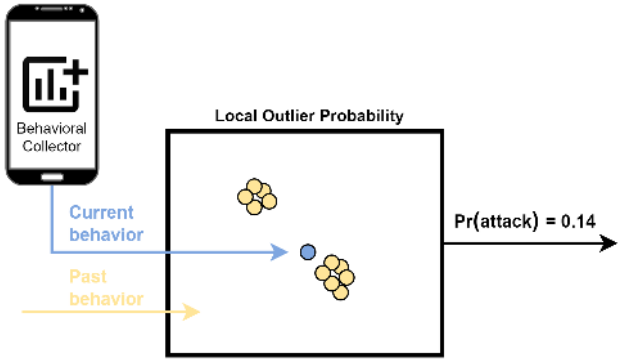
Dataset

The BehavioralCollector is publicly **available on Google Play**. Several groups of students were contacted via social media asking to use the app repeatedly for at least three days – the dataset should cover long-term use to enable behavioural drift analysis. The collected dataset used for data analysis contains data from **22 volunteers with 4 sessions** on average. Dataset includes 6 sensors and touch properties from a touchscreen.



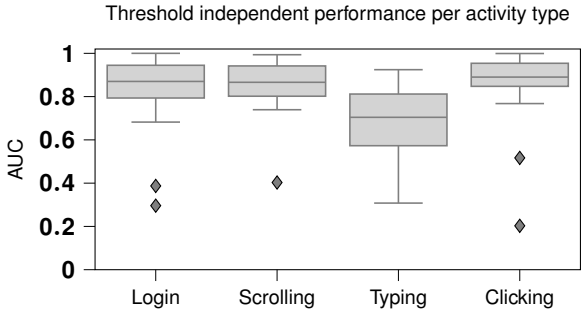
Evaluation of behavior

Newly captured behavioral characteristics are matched to past behavior using Local Outlier Probability model. It **outputs probability that the activity was performed by an attacker**.



These **outputs are then aggregated into a single probability**, that the whole session was performed by an attacker.

Results



The probabilities are aggregated using arithmetic mean, which outperformed Bayesian update approach. Equal Error Rate of the best performing data evaluation pipeline is 7 %. **The proposed authentication system is able to detect an attack based just on a user's behavior during an application interaction.**