ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

MA:

Fraud Detection in Mobile Payments

Mobile Payments are — much like credit card payments — often exposed to fraud and it is therefore important to pro actively and reactively prevent and detect fraud. Worldwide, the sum of credit card fraud is expected to be over 5.5bn$ annually. Existing ways of preventing and detecting fraud include black/white listing, credit limits, PIN Codes and more. As we get a lot more information from mobile payments than we usually get from credit card payments, there's a chance we can improve the detection and prevention by including more criteria like the digital signature, the gyro/accelerometer data, the GPS signal and a timestamp.

Examples could be:

- The signature of a buyer needs to match certain characteristics in order to be able to do the transaction.
- A merchant is only able to make transactions within its opening hours.
- Geo-Fencing - a merchant is only allowed to make transactions within a certain radius from its address, depending on the type of merchant (a taxi driver is allowed more distance than a grocery store)
- Adaptive limits - a transaction cant be higher than the maximum of the previous 50 transactions + 10%
- Collaborative Learning - If some transactions are marked fraudulent manually, the system learns about their characteristics and automatically flags transactions for different merchants and different buyers that show the same characteristics.

Requirements:
The student will work on location at the Startup. The student should be able to work independently on this topic.

Supervisors

- Christian Decker: cdecker@tik.ee.ethz.ch, ETZ G64.2