ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

MA/SA:

Design the next 2-factor authentication hardware

If you like to build custom hardware this might be just what you're looking for.

Mobile cashless payments are becoming increasingly popular. New means of payment include transactions issued from mobile phones, such as Google Wallet or Bitcoin. However, when money is involved the bad guys are never too far away. One can expect that in several years, smartphones will be as susceptible to spyware as PCs are today. The very ability to make payments wherever the phone is, makes it also possible for the funds to be stolen wherever it is.

One way to secure online payments is by using two-factor authentication. Some traditional options to implement this include sending an SMS to a registered phone number, looking up a security code on a list or adding a securely generated secret. When paying from mobile phones the SMS message does not add to the security. The list with security codes is cumbersome and has to be changed at regular intervals. Even with the hardware token the risk is, that what you think you are signing off, may not be what is really being authorized, if something is manipulating the display.

To allow for maximum security we need an unmodifiable environment that ensures not only that the secret is safe, but also that input and output are secure. Therefore we want **you** to build a simple hardware token that authenticates payment requests, received from the phone or even from the point-of-sale.

Don't hesitate to contact us for questions

Requirements: Experience in hardware prototyping. An interest in embedded system is advantageous. Independent problem solving skills.

Contacts

- Christian Decker: cdecker@tik.ee.ethz.ch, ETZ G64.2
- Samuel Welten: swelten@tik.ee.ethz.ch, ETZ G61.4