Secure Systems Group, Aalto University

N. Asokan

Securing Society with Platform Security

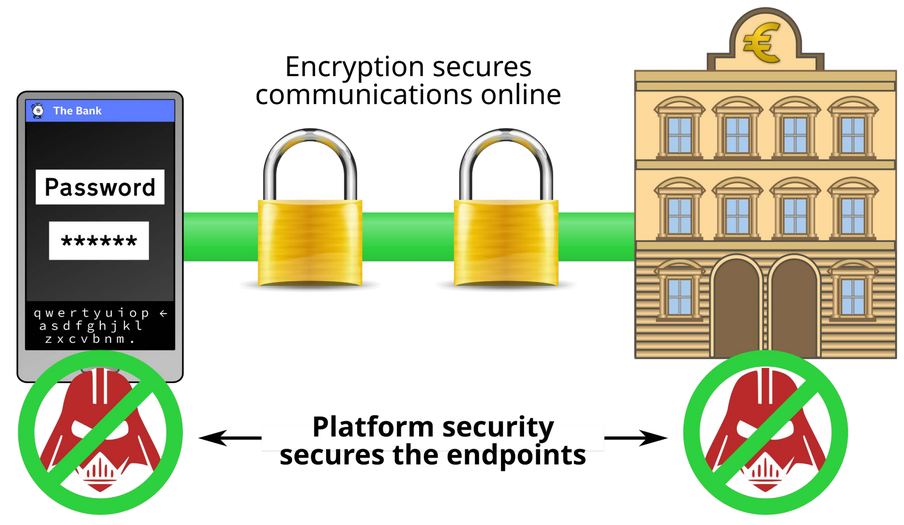
"… encryption on the Internet is like arranging an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench" - attributed to Gene Spafford

What?

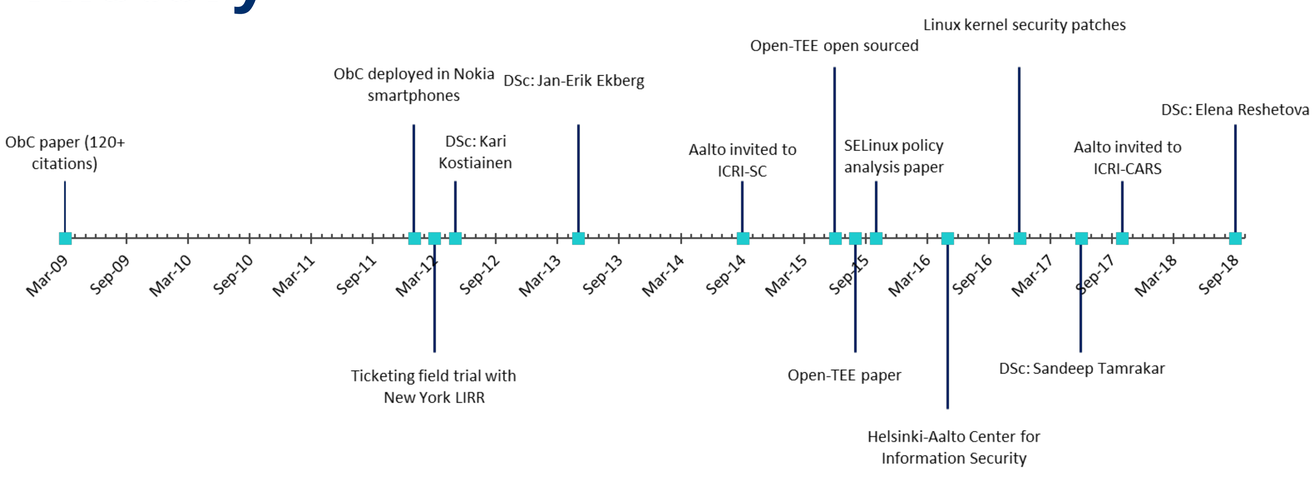
- Hardware and systems software technologies to secure applications and services

Why?

- Needed for true end-to-end protection



History



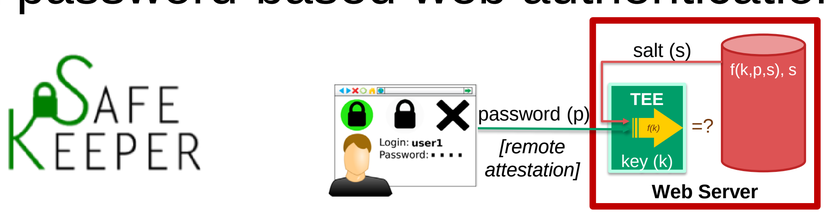
Achievements

Novel platform security technologies:

- **On-board Credentials**: first open platform for hardware-secured "trusted" applications (TA)
- **Open-TEE**: a TA development tool for standardized trusted execution environments

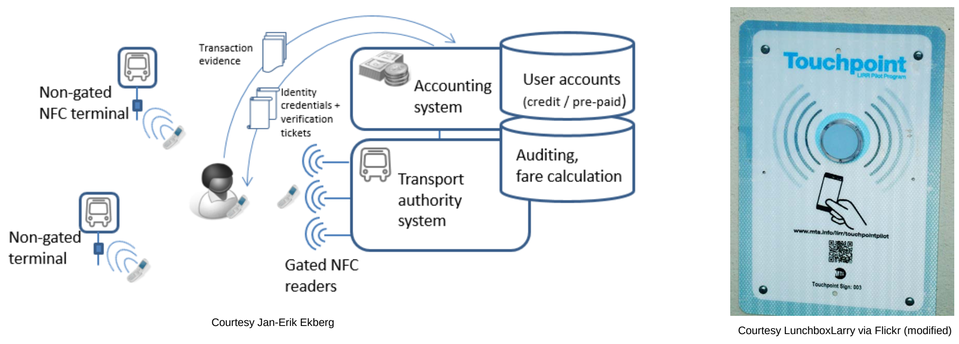
Examples of novel applications:

- Mobile ticketing (with Nokia)
- Securing password-based web authentication



Impact

- Ticketing trial on the NYC Long Island Rail Road



Courtesy Jan-Erik Ekberg

Courtesy LunchboxLarry via Flickr (modified)

- Open-TEE used by several companies
- 3 doctoral dissertations (+1 forthcoming)
- Over 10 MSc theses
  - 3 national thesis awards

Industry collaboration

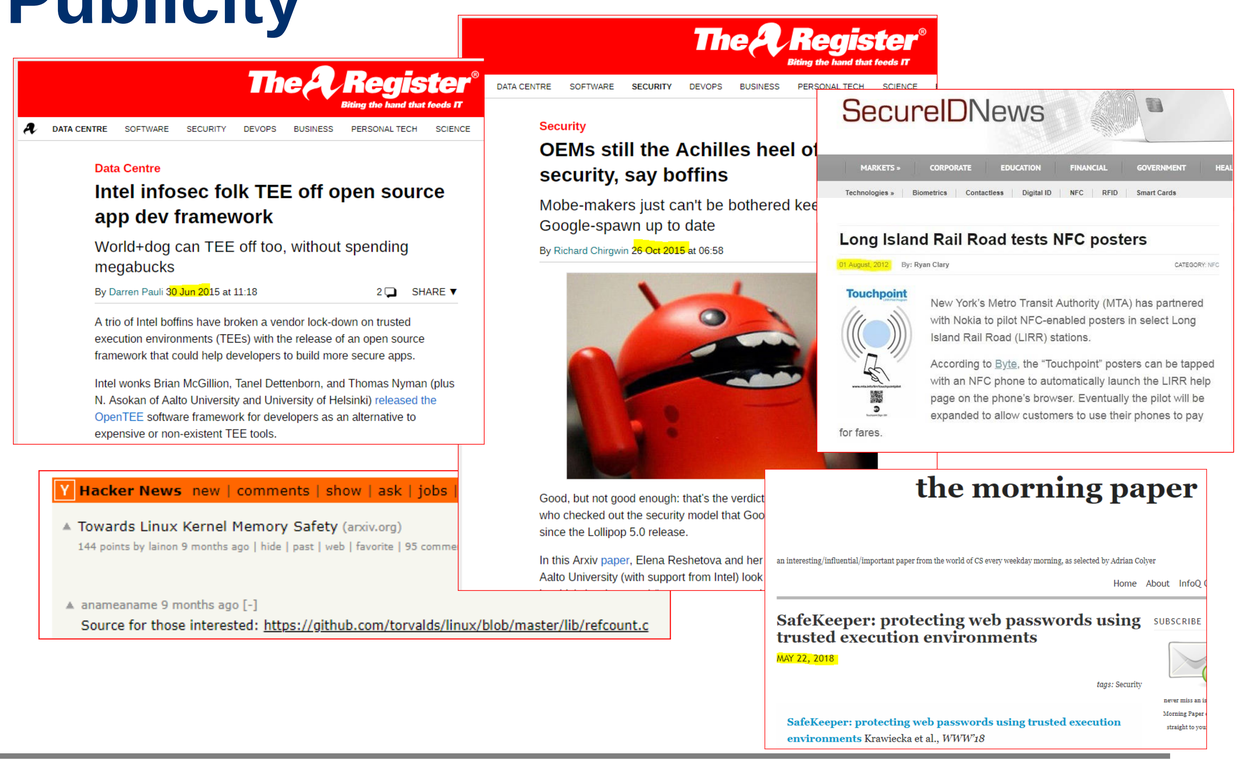
Nokia On-board Credentials:
2 industrial doctorates

Intel ICRI-SC & ICRI-CARS institutes
~1 M€ for systems security research at Aalto (2014-2020)
1 industrial doctorate

Trustonic Novel use cases for TAs

Huawei Hardware-assisted runtime protection

Publicity



Aalto University

https://ssg.aalto.fi/research/platsec /