Aalto University

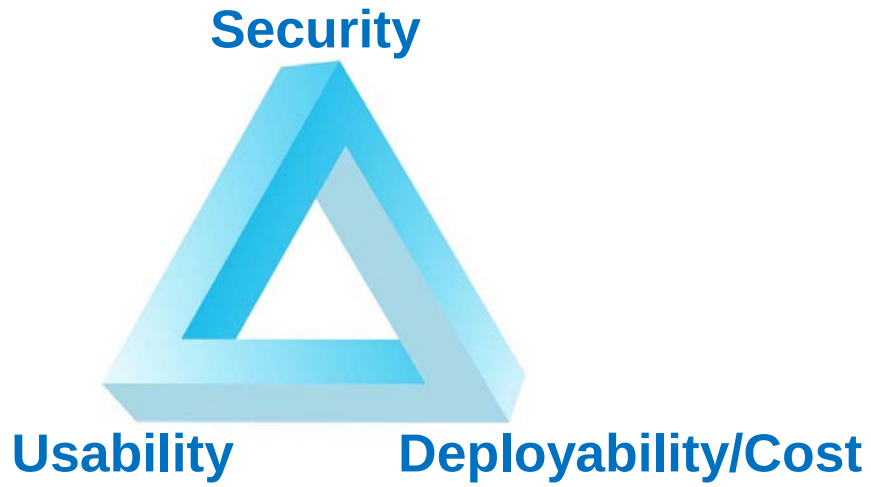
http://cs.aalto.fi/secure_systems/

Systems Security Research

N. Asokan

Secure Systems Group: Mission

How to make it possible to build systems that are simultaneously easy-to-use and inexpensive to deploy while still guaranteeing sufficient protection?



Secure Systems Group

http://cs.aalto.fi/secure_systems/

Two professors: Asokan and Aura

In Asokan's projects:

- 3 postdocs
- 5 full-time + 3 part-time PhD students

Several MSc students

- Best InfoSec thesis in Finland 2014 & 2016, Tietoturva ry
- Runner-up for Best CS thesis in Finland 2014, TKTS ry

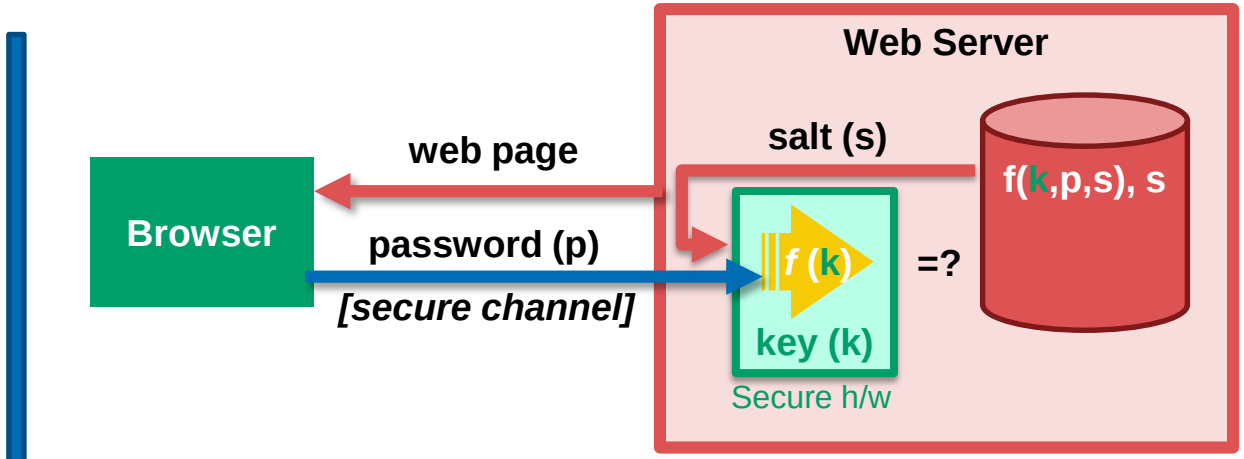
Projects funded by

- Academy of Finland, Tekes
- Direct industry support: E.g., Intel http://www.icri-sc.org, NEC Labs

Current themes: Platform Security

Enabling developers to secure apps/services using h/w and OS security

Example: SafeKeeper (Andrew Paverd's pitch talk and poster)



Use secure hardware on server side

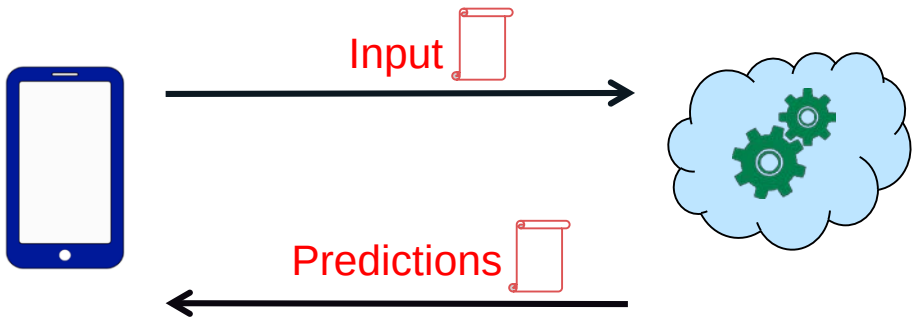
https://ssg.aalto.fi/projects/passwords/

SAFE KEEPER

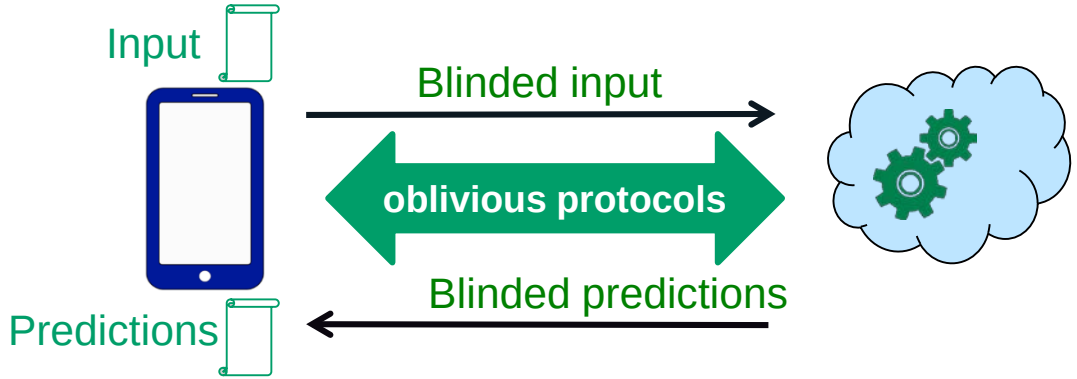
Current themes: Machine Learning & Security

Applying ML for Security & Privacy problems; Security & Privacy concerns in ML

Example: MiniONN (Jian Liu's pitch talk and poster)



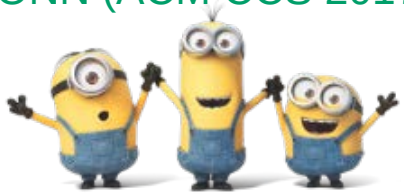
violates clients' privacy



Use inexpensive cryptographic tools

https://eprint.iacr.org/2017/452

MiniONN (ACM CCS 2017)



By Source, Fair use, https://en.wikipedia.org/w/index.php?curid=54119040

Current themes: Emerging topics

Distributed consensus and blockchains (theory, applications) [AoF project BCon, ICRI-SC]

- Can hardware security mechanisms help design scalable consensus schemes?

Securing IoT (scalability, usability) [AoF project SELIoT]

- How do we secure IoT devices from birth to death?

Security and privacy of vehicle-to-X (V2X) communication [ICRI-SC]

- How to reconcile privacy and lawful interception?

Stylometry and security [HICT scholarship]

- Can text analysis help detect deception?

ICRI-SC

Intel Collaborative Research Institute for Secure Computing

- **Only Intel Institute for security outside the US**

http://www.icri-sc.org/

ICRI-SC for mobile and embedded systems security

- **2012-2017 (Aalto, TU Darmstadt, UH; Aalto joined in 2014)**
- **Nearly 1 M€ invested in Aalto and UH**

ICRI-SC for autonomous systems security

- **2017-2020 (Aalto, TU Darmstadt, RU Bochum, U Luxembourg, TU Wien)**

intel Collaborative Research Institute for Secure Computing

Our role in the new ICRI-SC

Secure consensus mechanisms

- How to make consensus in autonomous systems more efficient/scalable?
  - First step: Scalable Byzantine Consensus via Hardware-assisted Secret Sharing https://arxiv.org/abs/1612.04997

Security and privacy of machine learning

- How to design ML systems resistant to evasion?
- How to identify and limit information leakage in ML systems?
  - First step: Oblivious Neural Network Predictions via MiniONN transformations https://eprint.iacr.org/2017/452

intel Collaborative Research Institute for Secure Computing

Aalto University

http://cs.aalto.fi/secure_systems/

Systems Security Research

N. Asokan