Aalto University

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Secure Systems Groups

Demo Day 2018

N. Asokan, Tuomas Aura, Chris Brzuska, Valtteri Niemi

“State of the Union”

Who are we?

Aalto University

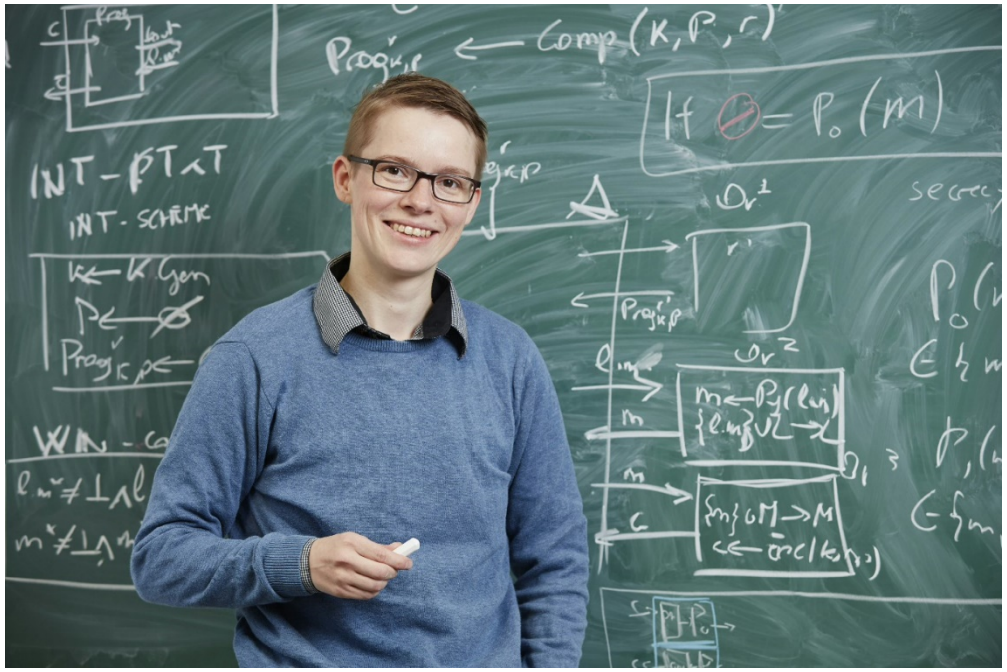
- **2 + 1 professors**
- **6 (4+2) postdocs**
- **Several PhD/MSc students and research interns**

University of Helsinki

- **1 Professor**
- **2 senior researchers**
- **2 postdocs**
- **Several PhD/MSc students**

New cryptology professor at Aalto

Prof Chris Brzuska started in April 2018



How are we funded?

3 Academy of Finland projects:

SecureConnect (autumn ’16 → autumn ’20), SELIoT (spring ’17 → autumn ’19), BCon (autumn ’17 → autumn ’20)

2 Tekes projects:

CloSer (autumn ’16 → autumn ’18), Take5 (autumn ’16 →)

Intel Institute for autonomous systems security (ICRI-CARS)

(autumn ’17 → autumn ’20, successor of ICRI-SC)

Other industry funding: Zalando research gift

Basic funding from universities (Aalto and UH)

What do we work on?

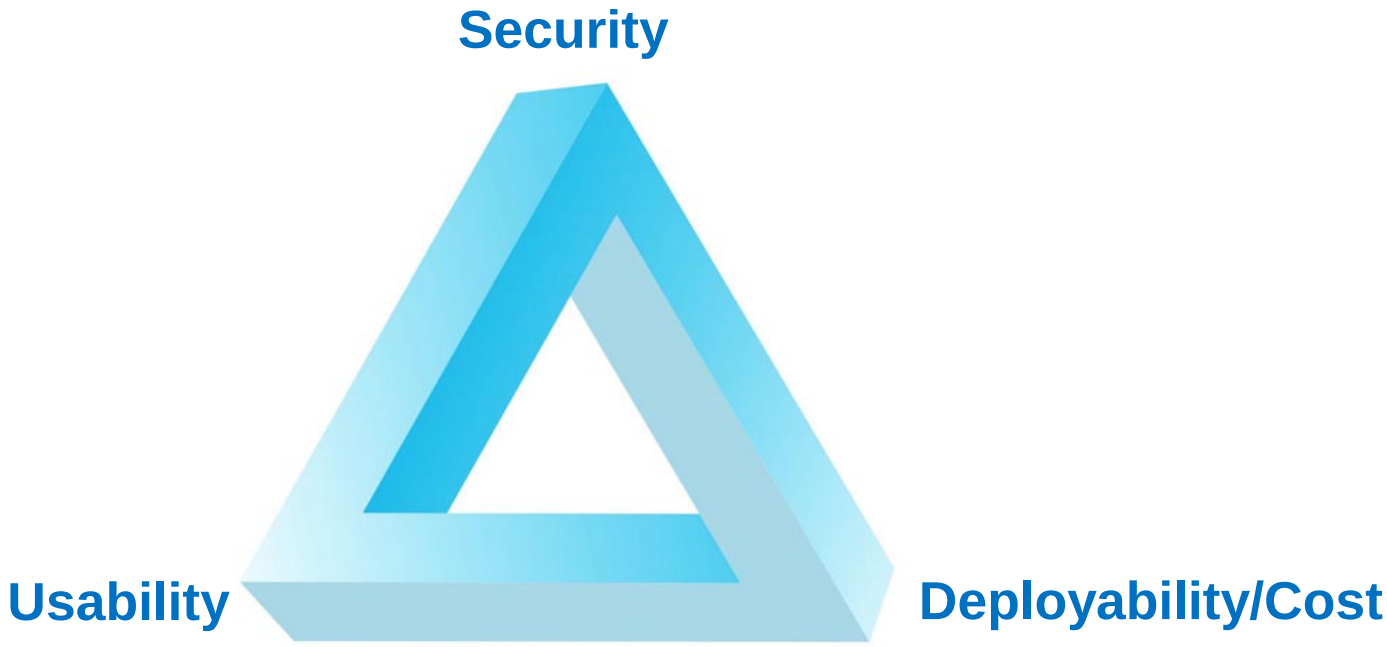
(Mobile) Platform Security
Machine Learning and Security
Other themes: Blockchains and consensus, Stylometry and security

5G Security

Security Protocol Engineering
Network Security
Security for Ubiquitous Computing

Protocol analysis: TLS, EMV, messaging
Formal verification
Foundations of cryptography
White-box cryptography

What do we work on?



Where are we publishing?

Top-tier infosec venues: ACM CCS, Usenix SEC

Other top-tier venues: WebConf, IEEE/ACM DAC, IEE TMC

Focused thematic venues: IEEE DSN

Other venues: CT-RSA, ESORICS, DefCon

What are we teaching?

Information Security courses

- **Bachelor level course on Information Security**
- **MSc level courses on network security, cryptography, mobile system security**
- **Seminar and laboratory courses**
- **MOOC: Cybersecurity Base with F-Secure**
- **Shared courses between Aalto and UH**

Courses taught by industry experts

- **Reverse Engineering Malware, Software Security (F-Secure)**

Recognition: **Two courses ranked among top-5 in Aalto CS department**
Best Infosec thesis in Finland, Runner up: Best CS thesis in Finland

~3M€ grant for three intakes; Scholarships available

secclo.aalto.fi **secclo@aalto.fi** **facebook.com/secclo**

Aalto University

DTU Technical University of Denmark

EURECOM

KTH

NTNU Norwegian University of Science and Technology

Tartu Ülikool

Co-funded by the Erasmus+ Programme of the European Union

Aalto University

UNIVERSITY OF HELSINKI

Helsinki-Aalto Center for Information Security, HAIC

Mission:
Attract top international master's students to Helsinki to specialize in information security

Activities:
Scholarships to top students donated by HAIC industry partners

Industry contacts: meet-and-greet events and company visits

Public outreach: HAIC Talks – lectures about information security + Annual Demo Days

http://haic.fi

HAIC in 2018

Spring 2018: Sustained collaboration with Finnish industry

New donations by F-Secure and Huawei (HAIC donors)

Group visits of HAIC students to partner companies

Summer 2018: 30 incoming MSc students

3 HAIC scholarships, 21 Erasmus Mundus scholarships

Demoday 2018: Enable companies to advertise opportunities to students

Company experts available to talk to students

Call to action: donors for next year

HAIC Public Outreach

Initiative launched in Autumn 2017 (Andrew Paverd appointed deputy director)

Three HAIC Talks so far

Yves Vandermeer

Moti Yung

Paul van Oorschot

More planned during Autumn 2018

Note: Yvo Desmedt's CS Forum talk on Monday, June 25.

“Demo/Poster Teasers”

Secure Systems Group, Aalto University:

- Thomas Nyman "**HardScope: Hardware-assisted Run-time Scope Enforcement**", poster + demo
- Tommi Gröndahl & Luca Pajola "**Evading hate speech detection**", poster
- Sebastian Szyller & Alexey Dmitrenko "**PRADA: Protecting against DNN Model Stealing Attacks**", ICRI-CARS project, poster + demo
- Max Reuter "**Privacy Preserving Deep Neural Network Prediction using Trusted Hardware**", ICRI-CARS project, poster
- Samuel Marchal "**DÏoT: A Crowdsourced Self-learning Approach for Detecting Compromised IoT Devices**", SELIoT project, poster
- Jian Liu "**Robust and efficient sharding for smart contracts**", BCon project, poster
- Tange Koen "**SACBFT: single active counter Byzantine fault tolerance**", BCon project, poster
- Shohreh Hosseinzadeh "**Control Flow Obfuscation to Mitigate Branch-Shadowing Attack on Intel SGX**", poster
- Siddhart Rao & Markku Antikainen "**Man-in-the-Machine (MitMa): Exploiting Ill-Secured Communication Inside the Computer**", poster
- Fritz Alder "**Migrating SGX Enclaves with Persistent State**", CloSer project, poster
- Arseny Kurnikov "**Cloud Key Store**", CloSer project, poster + demo
- Arseny Kurnikov "**SafeKeeper: Protecting Web Passwords using Trusted Execution Environments**", poster + demo
- Aleksi Peltonen "**Model Checking the EAP-NOOB Protocol**", poster
- Mika Juuti "**Stay On-Topic: Generating Context-specific Fake Restaurant Reviews**", poster + demo
- Lachlan Gunn & Ricardo Vieitez Parra "**Breaking and repairing deniable messaging using remote attestation**", poster
- Hans Liljestrand "**PARTS: Code- and Data-flow Integrity using ARM Pointer Authentication**", poster
- Mustafa Khalid "**Occupant identity leakage from CO2 sensors**", poster
- Mariia Kovtun "**Scalable Honeypot Monitoring and Analytics**", poster

Secure Systems Group, University of Helsinki:

- Sara Ramezanian & Tommi Meskanen "**Privacy-preserving graph searches**", poster + demo
- Andrey Shorov & Peter Karis "**5G testbed for network slicing security evaluation**", poster + demo
- Raine Nieminen & Kimmo Järvinen "**Privacy-protecting positioning mechanisms**", poster + demo
- Mohsin Khan "**Identity privacy in 5G, defeating downgrade attack**", poster
- Masoud Naderpour & Andrey Shorov "**Privacy-preserving carsharing for autonomous, connected cars**", poster
- Gizem Akman "**Providing Identity Privacy in 5G Networks using Pseudonyms**", poster + demo

Visitor groups:

- Rainhard Findling "**Mobile Match-on-Card Authentication Using Offline-Simplified Models with Gait and Face Biometrics**", poster. *Ambient Intelligence Group, Aalto University*
- Le Nguyen "**Representation Learning for Sensor-based Device Pairing**", poster. *Ambient Intelligence Group, Aalto University*
- Maxim Smirnov & Päivi Tynninen "**Clustering spam campaigns**", poster. *ITMO University / Aalto University / F-Secure*
- Amit Tambe "**A Scalable VPN-forwarded IoT Honeypot for COTS Devices**", poster. *Singapore University of Technology and Design* (SUTD)

Poster

Man-in-the-Machine (MitMa):

Exploiting ill-secured communication inside the computer

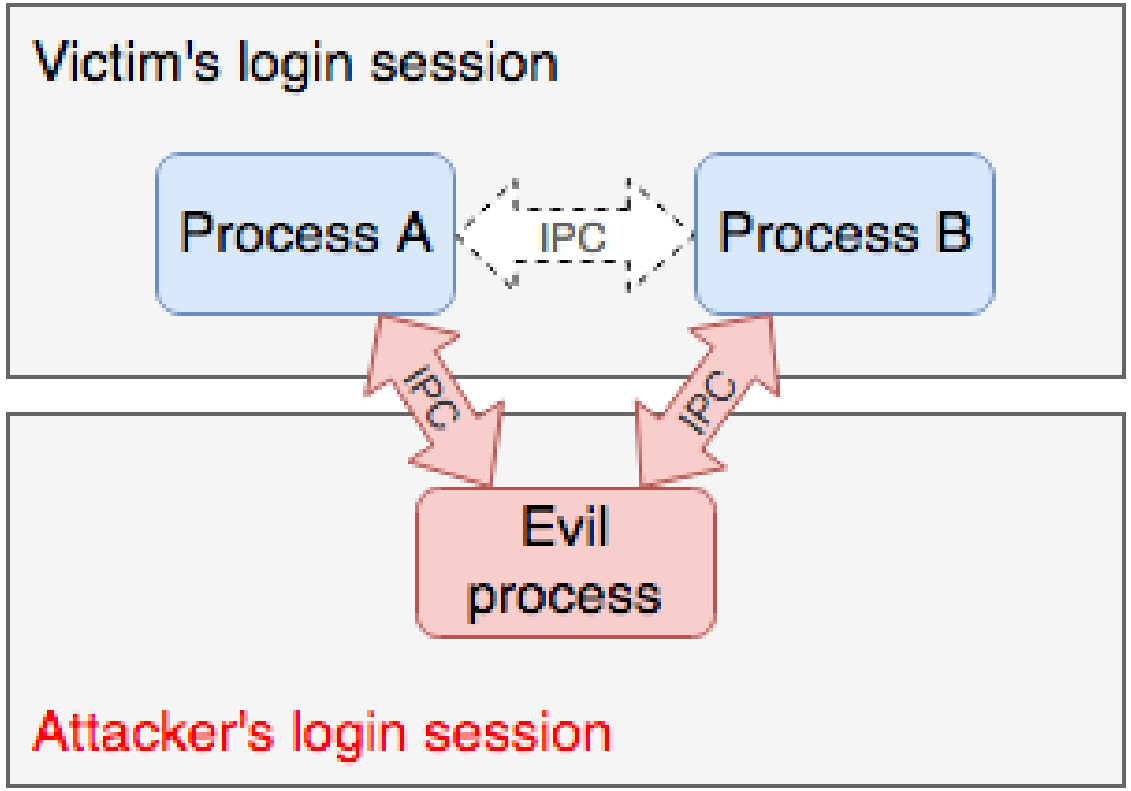
Modern software often consists of **separate frontend** and **backend components.**

The communication (IPC) between the components is often done insecurely

- Allowing non-privileged processes to access the communication channel

We find IPC-related vulnerabilities in several security critical apps

- Password managers, 2-factor hardware tokens etc.



The results have been accepted to USENIX Security 2018 and to DEF CON 2018.

SafeKeeper: protecting web passwords

Poster

Demo

Passwords are the most widely used authentication mechanism in the web.

They are not protected enough: phishing, brute-force attacks.

Passwords are weak secrets

- Phishing and password re-using
- Password database thefts

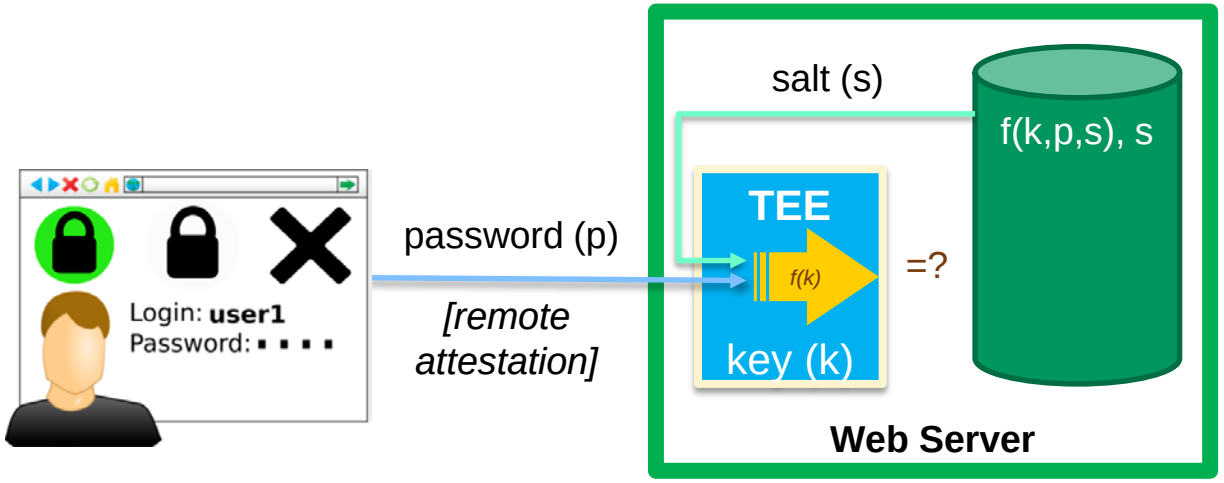
They are used everywhere

Using TEEs for server password protection

- Even against malicious server
- Rate limiting

Directly replace current mechanisms

- Deployability
- Scalability
- Easy upgrade



Winner, Best Infosec Thesis in Finland

Runner-up, Best CS Thesis in Finland

Breaking & repairing deniable messaging

Poster

Demo

Attestation can be used to undetectably break deniable messaging

Attestation can help restore deniability in messaging

Deniable messaging is useful…

- whistleblowers, marginalized, politicians,…

and popular

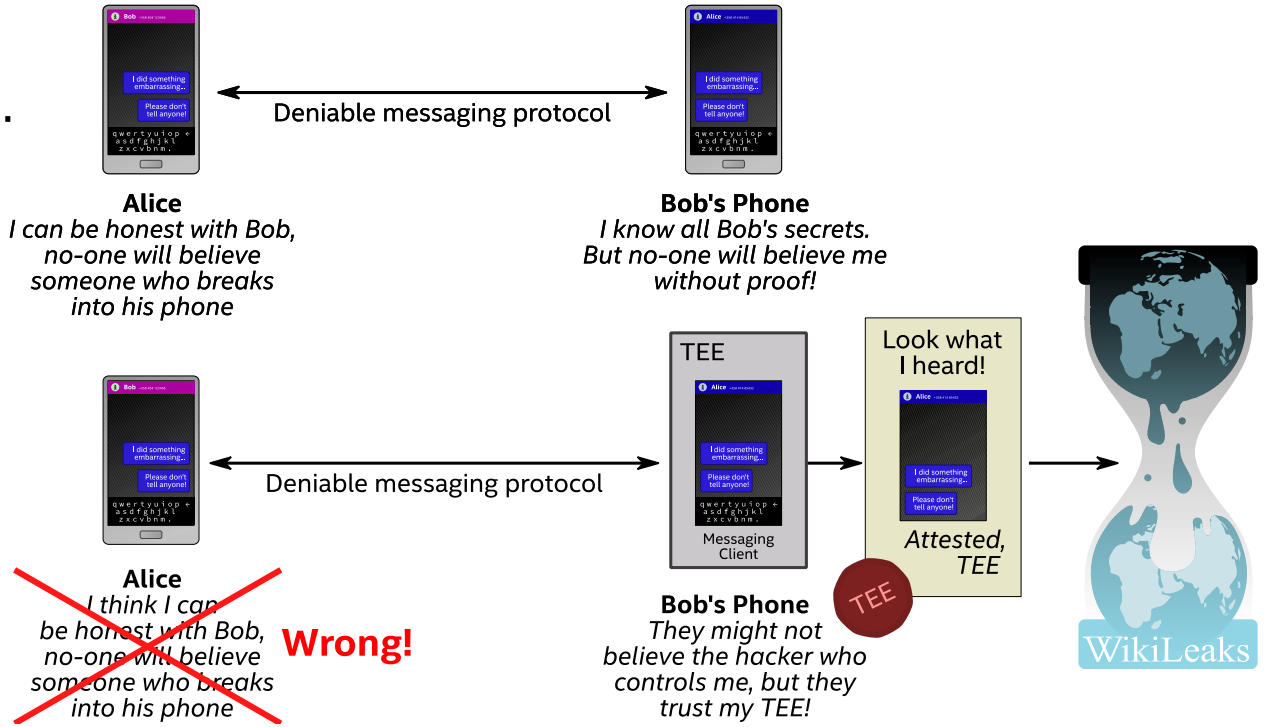
- Signal/WhatsApp, Telegram, OTR, …

Undetectably breaking deniability

- have TEE attest received messages to skeptical verifiers

S/W attacker: thwarted using attestation

- H/W attackers are hard to defend against



Poster

Demo

Stay On-Topic: Generating Context-specific Fake Restaurant Reviews

How close are we to creating **machine-generated** deceptive online text**?**

NMT-Fake* creates fake reviews from **description**:

- *5 Chipotle Mexican Grill Las Vegas NV Mexican Fast Food*

User study with **skeptical people**:

- Very poor detection, almost random (~53%)
- Detectable with machine learning (~97%)

Demo: generate your own fake restaurant reviews & discuss how to deal with threat

1, I have never had a bad experiance here. The staff is very nice, the place is clean and the portions are generous for what you're getting. *

Is this review a machine-generated fake review?

FAKE

- ○ Human-written
- ○ Machine-generated

2, Great! Chipotle is my favorite. This location is beautiful and close to home. Service is always on point and the food is awesome! *

Is this review a machine-generated fake review?

REAL

- ○ Human-written
- ○ Machine-generated

3, I love chipotle. It never fails me when I'm starving! I like the fact that they use free range meat. *

Is this review a machine-generated fake review?

REAL

- ○ Human-written
- ○ Machine-generated

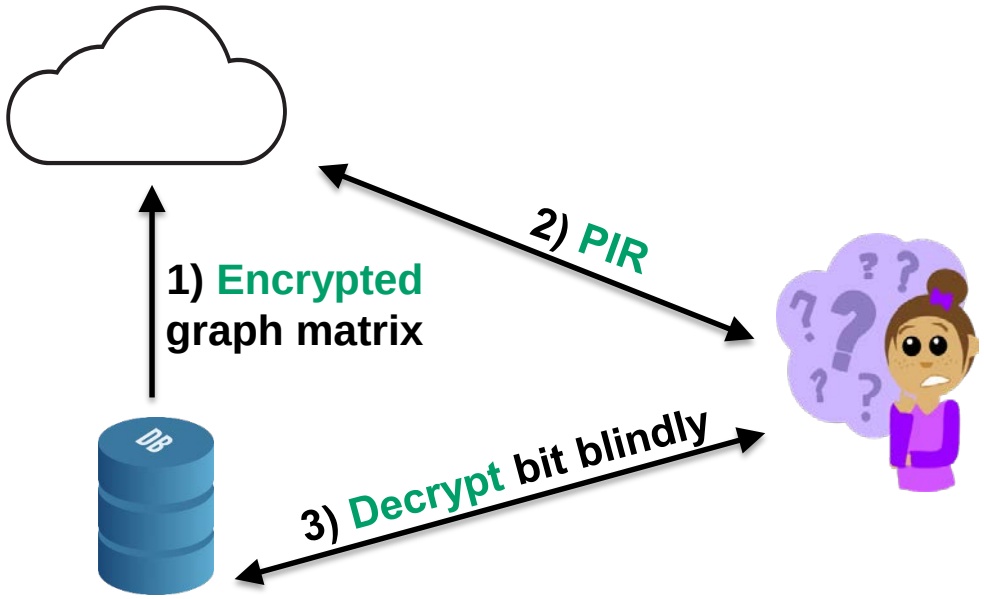
Poster

Demo

Privacy-preserving Graph Searches

How can an entity query the graph to find “if there is a path from A to B”, without sacrificing the privacy?

- Two lists of triplets: (user, host, fingerprint) and (fingerprint, user, host), define **trust relations** between users on different hosts.
- This database can be illustrated as a directed graph.
- The graph owner constructs the transitive closure of the directed graph (tc-graph) and stores the tc-graph into a matrix.
- There are three parties in this protocol: Owner of the graph, user and the Cloud.

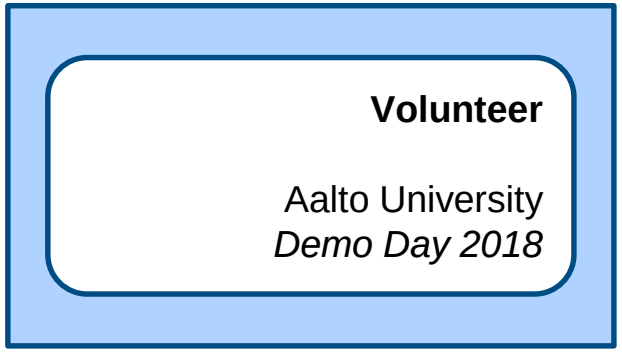


Logistics for the day

Logistics for today

Demos/posters downstairs at the library starting at 14:15

Follow volunteers



Coffee served by the library at 14:00 (refill at 16:00!)

Students: volunteers from companies are here to tell you about internships, thesis positions and other opportunities