Aalto University

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Secure Systems Groups

Demo Day 2019
N. Asokan, Tuomas Aura, Valtteri Niemi

“State of the Union”

Who are we?

Aalto University

- 2 + 1 professors
- 4 (3+1) postdocs
- Several PhD/MSc students and research interns

University of Helsinki

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

How are we funded?

3 Academy of Finland projects:

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

1 Business Finland project:

5G-FORCE (spring ’19 → autumn ’20)

2 EU projects:

FENTEC (autumn ’18 → spring ’21), HELIOS (Spring ’19 → autumn ’21)

Intel Institute for autonomous systems security (ICRI-CARS)

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

Other industry funding: research gifts from Zalando and Movial

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

Applied cryptography

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?

Security

Usability

Deployability/Cost

Where are we publishing?

Self evaluation: Good but room to improve

Top-tier infosec venues: Usenix SEC

Other top-tier venues: IEEE ICDCS, IEEE EMSOFT/TCAD IEEE/ACM DAC, IEEE TMC, IEEE JSAC, IEEE Trans. Computers, IEEE INFOCOM

Focused thematic venues: PETS

Other venues: BlackHat EU, IEEE Euro S&P, ACM ASIACCS

What are we teaching?

Information Security courses

- Bachelor level course on Information Security
- MSc level courses on network security, cryptography, mobile system security
- Research seminar: ML and 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: Best Infosec thesis in Finland

SECCLO

Master's Programme in Security and Cloud Computing

(Erasmus Mundus)

~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 VETENSKAP OCH KONST

NTNU Norwegian University of Science and Technology

TARTU ÜLIKOOL UNIVERSITAS TARTUENSIS 1632

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

@haic_fi haic.fi http://haic.fi

HAIC in 2019

Spring 2019: Sustained collaboration with Finnish industry

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

Group visits of HAIC students to partner companies

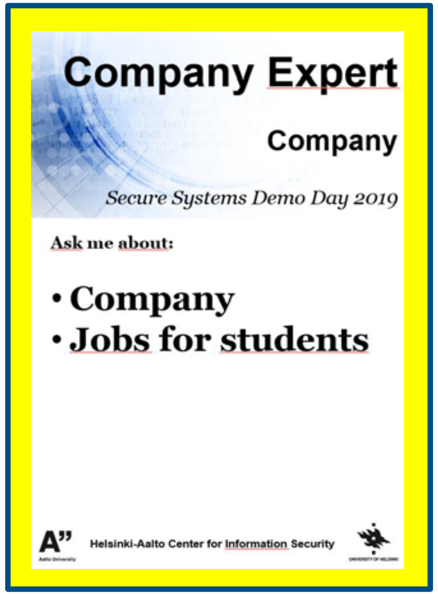
Summer 2019: 30 incoming MSc students

2-3 HAIC scholars, 21 Erasmus Mundus scholars

Demoday 2019: Enable companies to advertise opportunities to students

Company experts available to talk to students

Call to action: donors for next year



Company Expert

Company

Secure Systems Demo Day 2019

Ask me about:

- Company
- Jobs for students

Helsinki-Aalto Center for Information Security

HAIC Public Outreach

“Information security affects everyone”

Initiative launched in Autumn 2017

HAIC Talks: public lectures on contemporary topics in information security

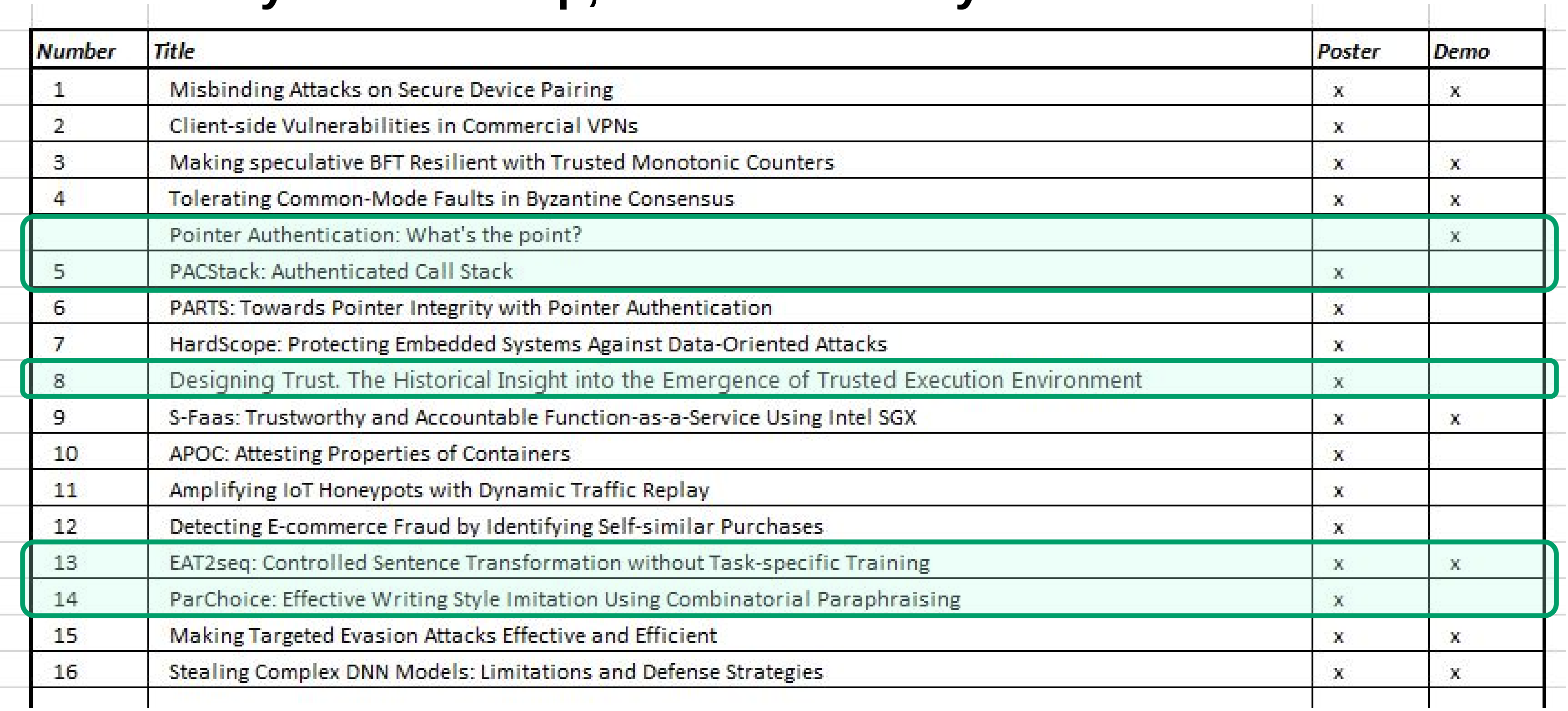
4 HAIC Talks since Demo Day 2018

https://haic.fi/talks/

March 1, 2019: 5G Security – the What, Why and How – with Alf Zugenmaier

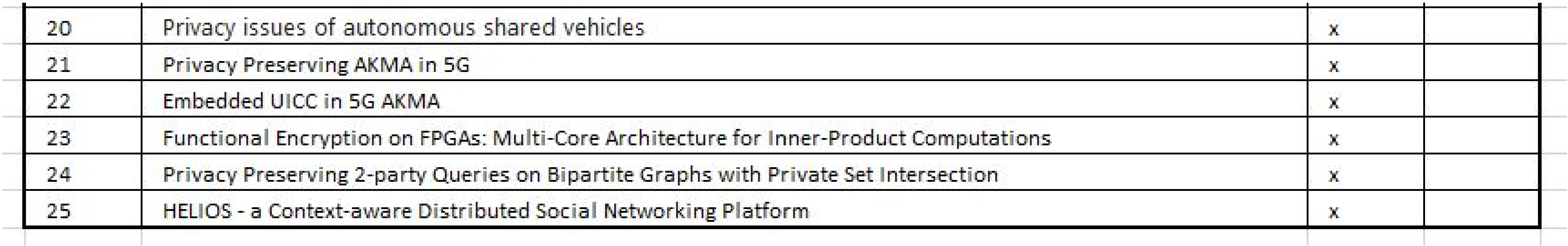
“Demo/Poster Teasers”

Secure Systems Group, Aalto University



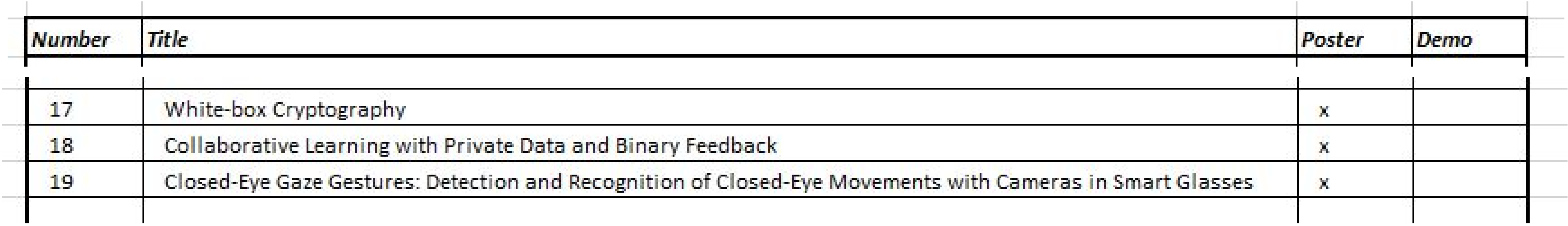
Number	Title	Poster	Demo
1	Misbinding Attacks on Secure Device Pairing	x	x
2	Client-side Vulnerabilities in Commercial VPNs	x	
3	Making speculative BFT Resilient with Trusted Monotonic Counters	x	x
4	Tolerating Common-Mode Faults in Byzantine Consensus	x	x
	Pointer Authentication: What's the point?		x
5	PACStack: Authenticated Call Stack	x	
6	PARTS: Towards Pointer Integrity with Pointer Authentication	x	
7	HardScope: Protecting Embedded Systems Against Data-Oriented Attacks	x	
8	Designing Trust. The Historical Insight into the Emergence of Trusted Execution Environment	x	
9	S-Faas: Trustworthy and Accountable Function-as-a-Service Using Intel SGX	x	x
10	APOC: Attesting Properties of Containers	x	
11	Amplifying IoT Honeypots with Dynamic Traffic Replay	x	
12	Detecting E-commerce Fraud by Identifying Self-similar Purchases	x	
13	EAT2seq: Controlled Sentence Transformation without Task-specific Training	x	x
14	ParChoice: Effective Writing Style Imitation Using Combinatorial Paraphraising	x	
15	Making Targeted Evasion Attacks Effective and Efficient	x	x
16	Stealing Complex DNN Models: Limitations and Defense Strategies	x	x

Secure Systems Group, University of Helsinki



20	Privacy issues of autonomous shared vehicles	x	
21	Privacy Preserving AKMA in 5G	x	
22	Embedded UICC in 5G AKMA	x	
23	Functional Encryption on FPGAs: Multi-Core Architecture for Inner-Product Computations	x	
24	Privacy Preserving 2-party Queries on Bipartite Graphs with Private Set Intersection	x	
25	HELIOS - a Context-aware Distributed Social Networking Platform	x	

Visitors: Cryptography group & Ambient Intelligence group, Aalto University



Number	*Title*	*Poster*	*Demo*
17	White-box Cryptography	x	
18	Collaborative Learning with Private Data and Binary Feedback	x	
19	Closed-Eye Gaze Gestures: Detection and Recognition of Closed-Eye Movements with Cameras in Smart Glasses	x	

Change is Constant

N. Asokan

Professor and Cheriton Chair at University of Waterloo, from September 2019

Adjunct Professor, Aalto University (Sep 2019 – Aug 2024)

- **Mobile Systems Security course, Spring 2020**
- **Graduating remaining doctoral students**
- **…**

Janne Lindqvist

Currently, Associate Professor, Rutgers
https://www.lindqvistlab.org/

Appointed Associate Professor at Aalto, from Jan 2020

HCI, security engineering, …

Director of HAIC, from Jan 2020

Will visit Aalto in Fall 2019

Jan-Erik Ekberg

Appointed (part-time) Adjunct Professor from Nov 2018

Platform security

Lachlan Gunn

Appointed Secure Systems Group co-leader, from Sep 2019

Responsible for leading the “Platform security” theme

Samuel Marchal

Appointed (part-time) Research Fellow, from Sep 2019

Responsible for leading the “Machine Learning and Security” theme

Systems Security Professor-of-Practice

On-going call for Professor-of-Practice (5-year term)

Decision expected in Autumn 2019

Logistics for the day

Logistics for today

For all:

Demos/posters downstairs at the library starting at 14:00

Follow volunteers

Coffee served by the library during the afternoon

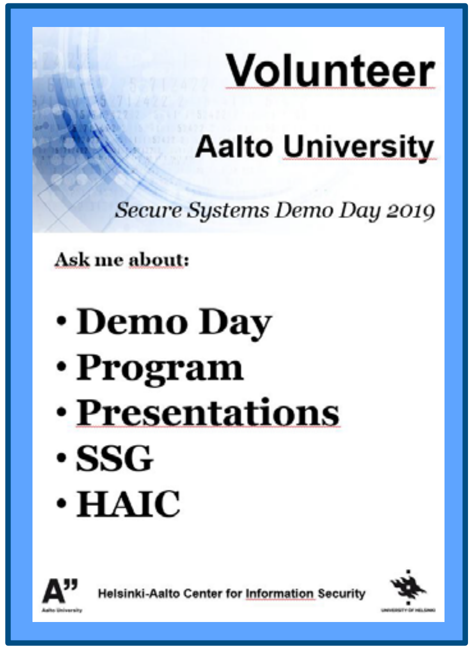
For students:

Volunteers from companies are here to tell you about

internships

thesis positions

other opportunities



Volunteer

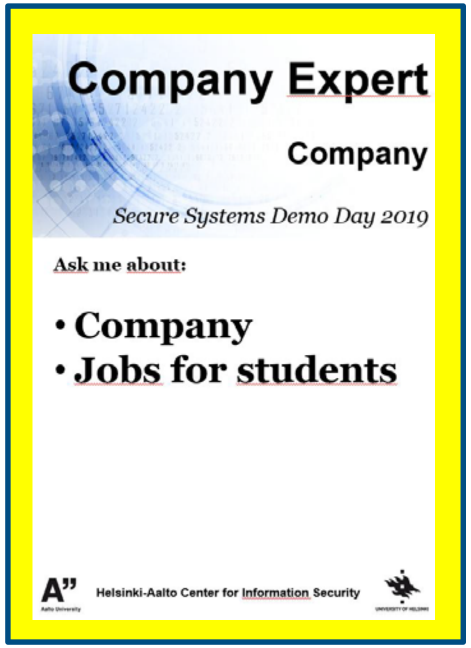
Aalto University

Secure Systems Demo Day 2019

Ask me about:

- Demo Day
- Program
- Presentations
- SSG
- HAIC

Helsinki-Aalto Center for Information Security



Company Expert

Company

Secure Systems Demo Day 2019

Ask me about:

- Company
- Jobs for students

Helsinki-Aalto Center for Information Security