Aalto University

Secure Systems Demo Day 2024

Presented by Lachlan Gunn

https://ssg.aalto.fi/

Aalto University

UNIVERSITY OF HELSINKI

Program:

14:00-15:00
Lecture Hall T1

Welcome
by Lachlan Gunn

Cybersecurity at VTT – Research Overview
by Samuel Marchal

15:00-18:00
CS Library
Poster session & thesis and job opportunities for students

17:00-18:00
CS Library
Dinner (Pizza)

Helsinki-Aalto Institute for Cybersecurity (HAIC)

Unique security ecosystem connecting students, academia and industry

Aalto University

UNIVERSITY OF HELSINKI

SSH

- Excellence in research and teaching
- Popular security MSc programmes
- Company donated HAIC scholarships for top students
- Forerunner in industrial interaction for students during studies
- Active community of information security specialists and students

Upcoming events

12.9.2024

HAIC x HelSec September 2024 Meetup

25.9.2024

HAIC Talk: Matthew Sorell, *University of Adelaide, Australia*

29.10.2024

HAIC Talk: Rain Ottis, *Tallinn University of Technology*

Aalto University

		Periods	ECTS
CS	**Information Security**	I	5
CS	**Network Security**	II	5
ELEC	**Basic principles in Networking**	III-IV	5
CS	**Platform Security**	III-IV	5
CS	**Cryptography**	I-II	5
CS	Special Course: **Advanced Cryptography**	I-II	5
CS	**Applied Cryptography**	III-IV	5
CS	**Seminar in Computer Science**	III-IV	5

CS	**Security Engineering**	III-IV	5	Updated
CS	Special Course in Information Security: **Malware Analysis and Engineering**	II	5	
ELEC	**Ambient Intelligence**	III-IV		
CS	**Cybersecurity Management**	III-IV	5	New!

Johdatus Kryptografiaan, MOOC

Introductory course on cryptography for lukio students

Cryptography in Networking

Trustworthy Machine Learning

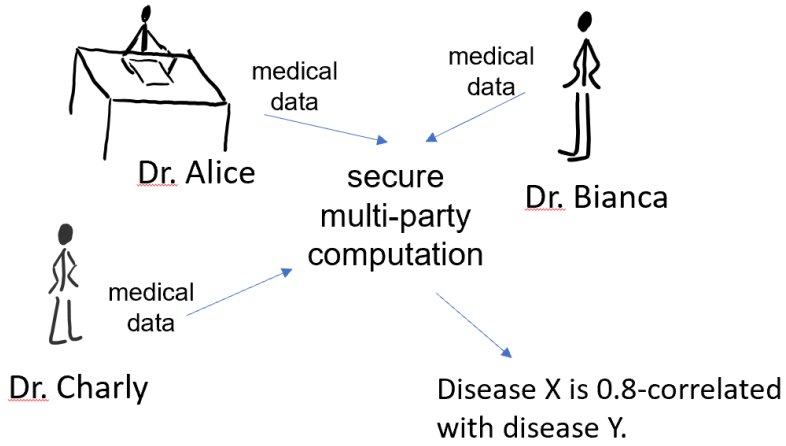
UNIVERSITY OF HELSINKI

Cyber Security Base with F-Secure: MOOC

Research Groups

Crypto @ Aalto: Chris Brzuska

Secure multi-party computation [1,2]
Formal verification [2]
Side-channel analysis [3]



[1] **Adaptive Distributional Security for Garbling Schemes**
E. Alpirez Bock, C. Brzuska, P. Karanko, K. Puniamurthy
Asiacrypt 2023

[2] **A State-Separating Proof for Yao's Garbling Scheme**
C. Brzuska, S. Oechsner
Computer Security Foundations Symposium (CSF) 2023

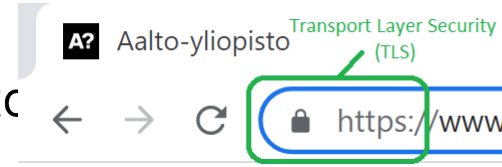
[3] **Breaking DPA-Protected Kyber via the Pair-Pointwise Multiplication**
E. Alpirez Bock, G. Banegas, C. Brzuska, L. Chmiliewski, K. Puniamurthy
Applied Cryptography and Network Security 2024

Courses 2024-2025:

- CS-E4340 Cryptography D (Period I-II)
- CS-EJ4404 Johdatus kryptografiaan (MOOC)

Looking for master students in

- formal verification & protocol analysis
- foundations of crypto



Crypto @ Aalto: Russell Lai

Selected publications:

- Post-quantum proof systems and signatures [1,2,3,4]
- Universal composability of cryptographic protocols [5,6]

1. Valerio Cini, Russell W. F. Lai, Giulio Malavolta, **Lattice-Based Succinct Arguments from Vanishing Polynomials** - (Extended Abstract). CRYPTO (2) 2023: 72-105
2. Russell W. F. Lai, Giulio Malavolta, **Lattice-Based Timed Cryptography**. CRYPTO (5) 2023: 782-804
3. Thomas Attema, Serge Fehr, Michael Klooß, **Fiat-Shamir Transformation of Multi-Round Interactive Proofs** (Extended Version). J. Cryptol. 36(4): 36 (2023)
4. Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Emmanuela Orsini, Lawrence Roy, Peter Scholl, **Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head**. CRYPTO (5) 2023: 581-615
5. Valerie Fetzer, Michael Klooß, Jörn Müller-Quade, Markus Raiber, Andy Rupp, **Universally Composable Auditable Surveillance**. ASIACRYPT (2) 2023: 453-487
6. Robin Berger, Brandon Broadnax, Michael Klooß, Jeremias Mechler, Jörn Müller-Quade, Astrid Ottenhues, Markus Raiber, **Composable Long-Term Security with Rewinding**. TCC (4) 2023: 510-541

Courses 2024-2025:

- CS-E4380 Special Course: Advanced Cryptography D (Period I-II)
- CS-E4370 Applied Cryptography D (Period III-IV)

Crypto @ Aalto: General

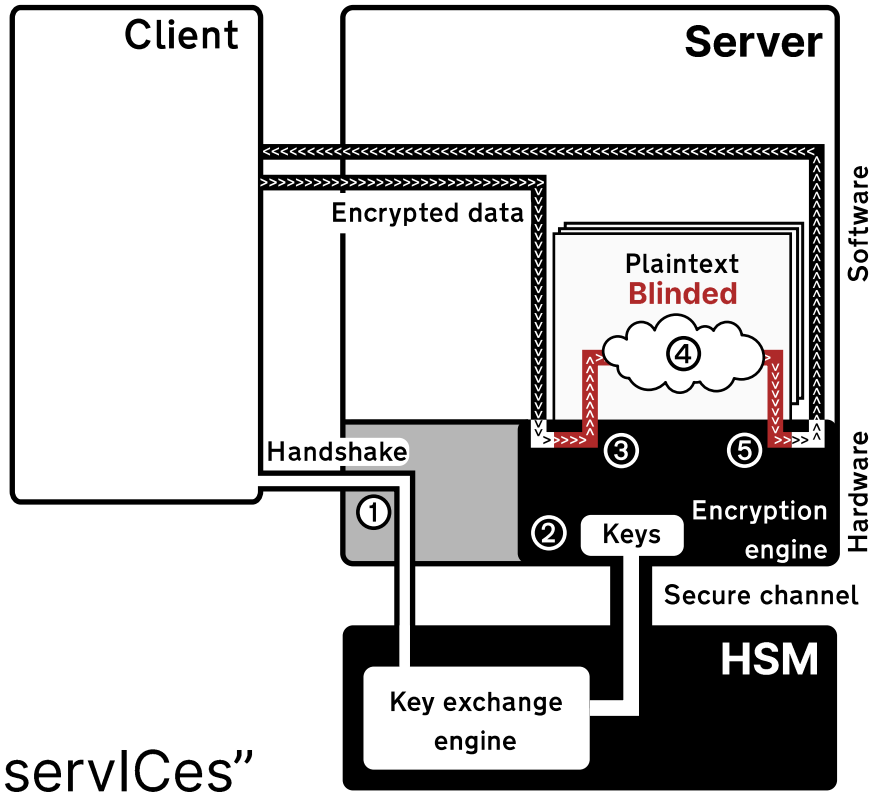
Ad: Looking to hire postdocs in areas including, but not limited to:

- Lattice-based cryptography
- Proof & argument systems
- Fine-grained cryptography
- Lower bounds and impossibility

Secure Systems @ Aalto: Lachlan Gunn

Run-time security mechanisms

- Architectures for secure outsourced computation
- Secure sandboxing with WebAssembly



Most interesting paper:

BliMe: Verifiably Secure Outsourced Computation with Hardware-Enforced Taint Tracking

Hossam ElAtali, Lachlan J. Gunn, Hans Liljestrand, and N. Asokan,
Network and Distributed Systems Symposium (NDSS) 2024

elacotic: **new EU HORIZON project**

"Efficient, portabLe And Secure orchesTration for reliable servICes"

Research Council of Finland: Rigorous security guarantees for run-time integrity

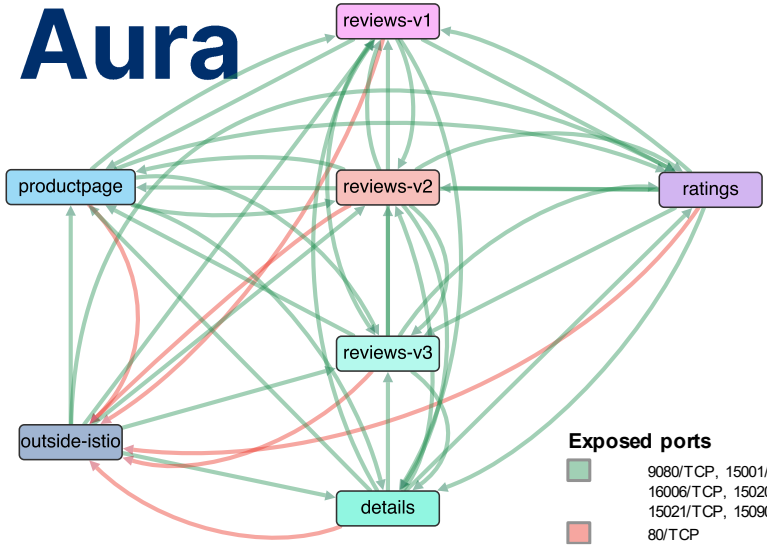
Ad: Looking to hire a doctoral student to work on platform security topics
esp. sandboxing, trusted execution environments, attestation

Secure Systems @ Aalto: Tuomas Aura

Cloud security policies

- Hardening Kubernetes cluster networks to limit lateral movement of attackers

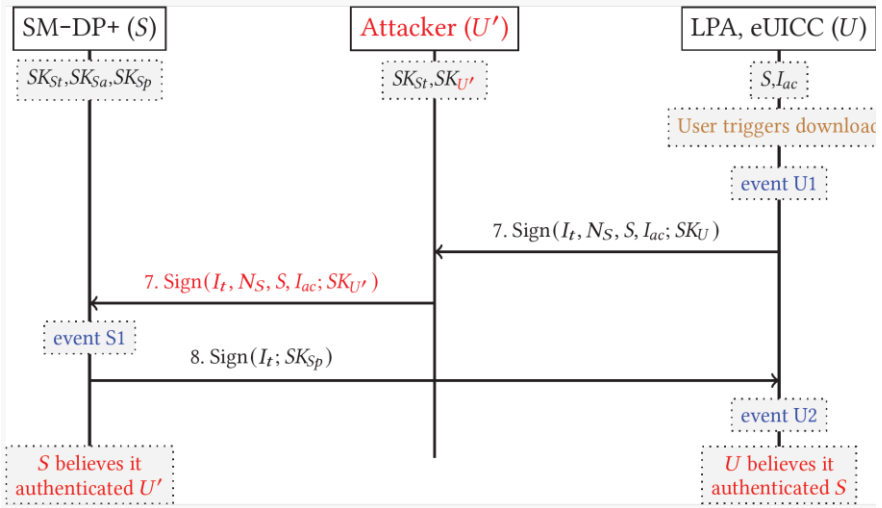
Jacopo Bufalino, Mario Di Francesco, and Tuomas Aura. Analyzing Microservice Connectivity with Kubesonde. ESEC/FSE 2023



Security protocols

- Protocol modeling and verification

Abu Shohel Ahmed, Aleksi Peltonen, Mohit Sethi, and Tuomas Aura. Security Analysis of the Consumer Remote SIM Provisioning Protocol. ACM Trans. Priv. Secur. 2024.



Funding: Research Council of Finland project: Isolation in modern networks and services
Cybersecurity PoP donated by Xamk, city of Kotka and others

Secure Systems @ Aalto: Janne Lindqvist

Two exciting posters:

Amel Bourdoucen, Janne Lindqvist

Privacy of Default Apps in Apple's Mobile Ecosystem. CHI 2024: 786:1-786:32

Amel Bourdoucen , Leysan Nurgalieva , Janne Lindqvist

Privacy Is the Price: Player Views and Technical Evaluation of Data Practices in Online Games. Proc. ACM Hum. Comput. Interact. 7(CHI): 1136-1178 (2023)

Secure Systems @ Aalto: Sanna Suoranta

Security and Usability

- How common users can cope with computer security

Current work:

- **How user interface elements affect the choices users make**
- **Incoming call authentication**
- Dark patterns in TikTok and engagement
- Usability of multi-factor authentication

Secure Systems Group @ University of Helsinki

Demos:

- Fake base station detection (**Sanish Gurung**)
- Privacy-aware fair meeting point selection (**Taoufiq Damir**)

Posters:

- Privacy-preserving Location-based advertising with fine-grained statistics (**Gizem Akman**)
- FBS detection with Open RAN (**Amy Sidibé**)
- Cybersecurity education network in Finland (**Harri Kähkönen**)

Projects:

- (Security in) 6G test network Finland
- Cybersecurity Education Development,
- Privacy-aware Location-based services
- Secure Enclave Migration

Selected papers:

- Gizem Akman, Mohamed Taoufiq Damir, Philip Ginzboorg, Sampo Sovio, Valtteri Niemi
  Split Keys for Station-to-Station (STS) Protocols.
  Journal of Surveillance, Security and Safety 2023
- Philip Ginzboorg, Valtteri Niemi, Jörg Ott
  Authentication of Fragments with Short Tags
  Theoretical Computer Science 2024

Doctoral defences since last demo day

Abu Shohel Ahmed, Advancing authentication for cellular networks and mobile users, Aalto 2023-08-02

Aleksi Peltonen, Formal Verification and Standardization of Security Protocols, Aalto 2023-08-08

Siddharth Prakash Rao, Analyzing Communications and Software Systems Security, Aalto 2023-08-28

Konrad Kohbrok, State-Separating Proofs and Their Applications, Aalto 2023-08-10

Georgios Giantamidis, On Pragmatic System Design through Learning and Implementation-oriented Reachability Analysis, Aalto 2023-08-30

Ameet Gadekar, Parameterized Approximation Results for Clustering and Graph Packing Problems, Aalto 2024-01-25

Sebastian Szyller, Ownership and Confidentiality in Machine Learning, Aalto 2023-08-18

Best doctoral thesis award, 2023

Demo Day

Posters

Too many to list legibly this year!

Please join us in the library

- **Poster session: 15.00-18.00**
- **Dinner: Pizza arriving around 17.00**

- Privacy of Default Apps in Apple's Mobile Ecosystem
- Privacy Is the Price: Player Views and Technical Evaluation of Data Practices in Online Games
- Image geolocation
- Implementation of GlobalPlatform TPS keystore using OPTEE
- Establishing Trusted Channels for Confidential Workloads
- Implementation of split-key protocols for secure enclaves
- Improving Static Analysis Reporting with Large Language Models
- REST API Security Testing within the IEC-62443-4-1 Standard
- Policy generation and misconfiguration abuse in Kubernetes networks
- Helm-ET: Reducing Exposure to Lateral Movement in Kubernetes Artifacts
- Electronic voting with revocation
- On Resource Consumption of Distributed Machine Learning in Network Security
- Cyber Threat Intelligence for Security Operation Centres (SOCs) and Surveillance Technology: A literature review
- Formal Modelling of Blinded Memory in a System-on-Chip
- ML Property Attestation using TEEs
- Security for AI/ML in RAN applications
- Accept all cookies? Eye-tracking studies of cookie consent forms
- Formal models of key exchange with raw public keys
- Fake Base Station Detection
- Anonymous Location-based Advertising with Fine-Grained Statistics
- Privacy-Preserving Fair Meeting Point Agreement
- Network for Cybersecurity Education in Finland
- Double-edged sword: Exploring DoS attacks using CDN
- Multi-Platform Attestation Verification
- Authenticating and Authorizing the Caller: A Defense Mechanism Against Caller ID spoofing
- Covert watermarking of digital documents

Best Poster Award

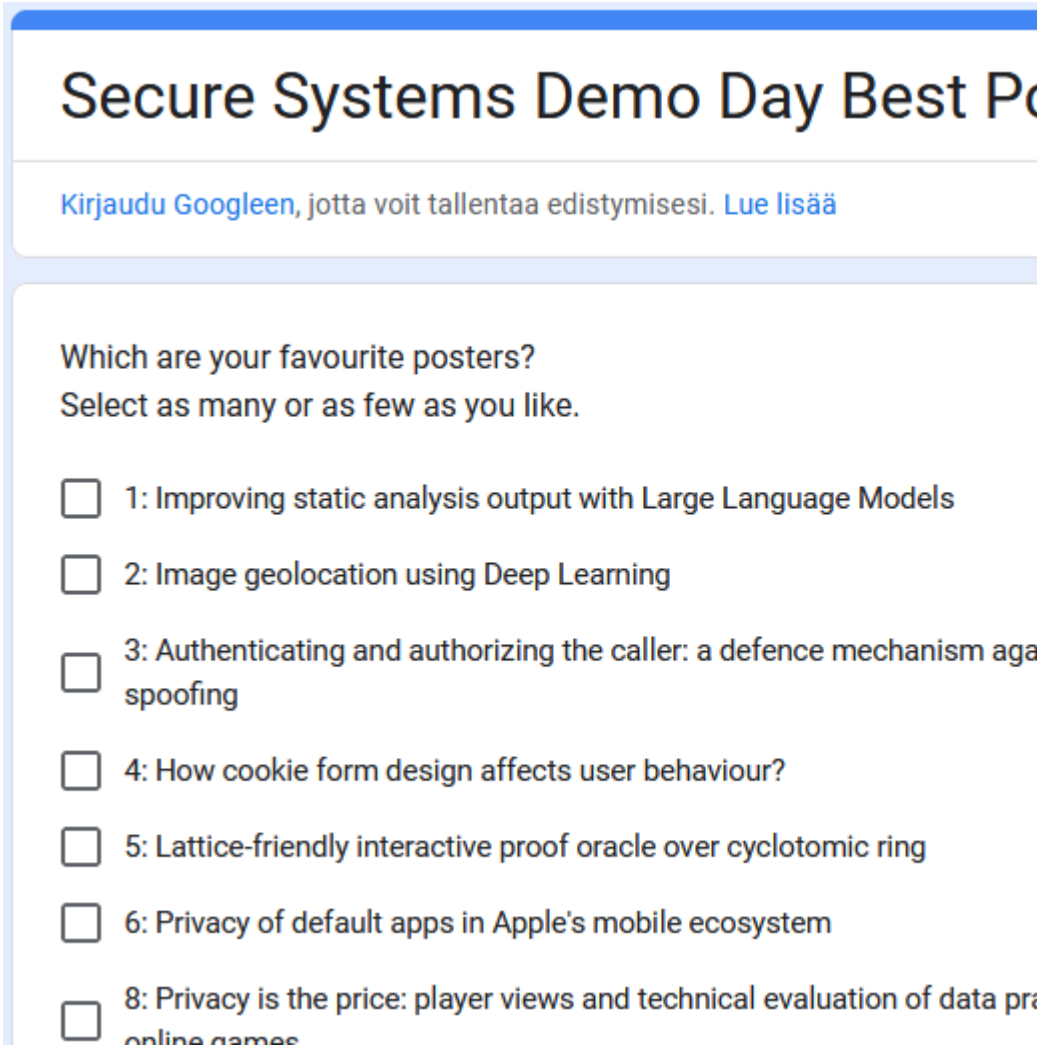
New this year!

Use the link below to vote

- Vote for as many posters as you like
  - You can edit your vote
- Most total votes wins

Voting ends when the pizza arrives at 17
Results announced shortly afterwards

forms.gle/TdJTiVdjE73GCEhBA



Company desks

Housekeeping notes

Toilets are on the 2nd and 3rd floor (1st floor toilets not in use)

Catering

- Coffee & buns at 15
- Pizza at ~17

Metro station: Exit B (Tietotie exit) NOT in use!

- Other entrance in A Bloc
- If you’re not sure, go towards the closed entrance and follow the detour sign

Name tags:

- Pick up downstairs if you don’t already have one
- Please return before you leave, thank you