Aalto University

Information Security Research and Education at Aalto

N. Asokan

http://asokan.org/asokan/

@nasokan

About me

Professor, Aalto University, from Aug 2013

Professor, University of Helsinki, 2012-2017

IEEE Fellow (2017), ACM Distinguished Scientist (2016)

Associate Editor-in-Chief, IEEE Security & Privacy (2017)

Previously

Nokia (14 y; built up Nokia security research team)

IBM Research (3 y)

https://asokan.org/asokan/ for more background

Secure Systems Group

Prof N. Asokan

Professor, Department of Computer Science

Director: Helsinki-Aalto Center for Information Security

http://asokan.org/asokan/

Prof Tuomas Aura

Professor, Department of Computer Science

Director: SECCLO joint degree program

https://people.aalto.fi/tuomas_aura

Dr Andrew Paverd

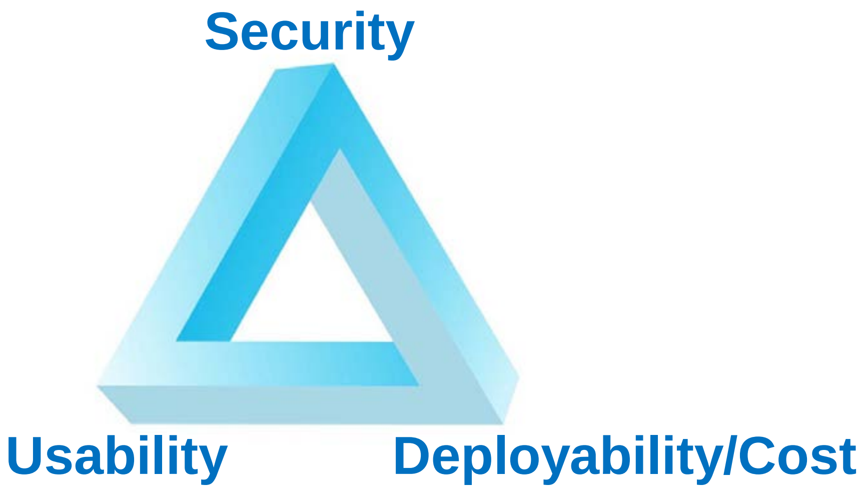
Research Fellow, Department of Computer Science

Deputy Director: Helsinki-Aalto Center for Information Security

https://ajpaverd.org

Secure Systems Group

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



Security

Usability

Deployability/Cost

Research

Building systems that are secure, usable, and deployable

Current major themes

Platform Security

- How can we design/use pervasive hardware and OS security mechanisms to secure applications and services?

Machine Learning & Security

- Can we guarantee performance of machine-learning based systems even in the presence of adversaries?

Research: Platform Security

Platform security: overview

Applications of platform security

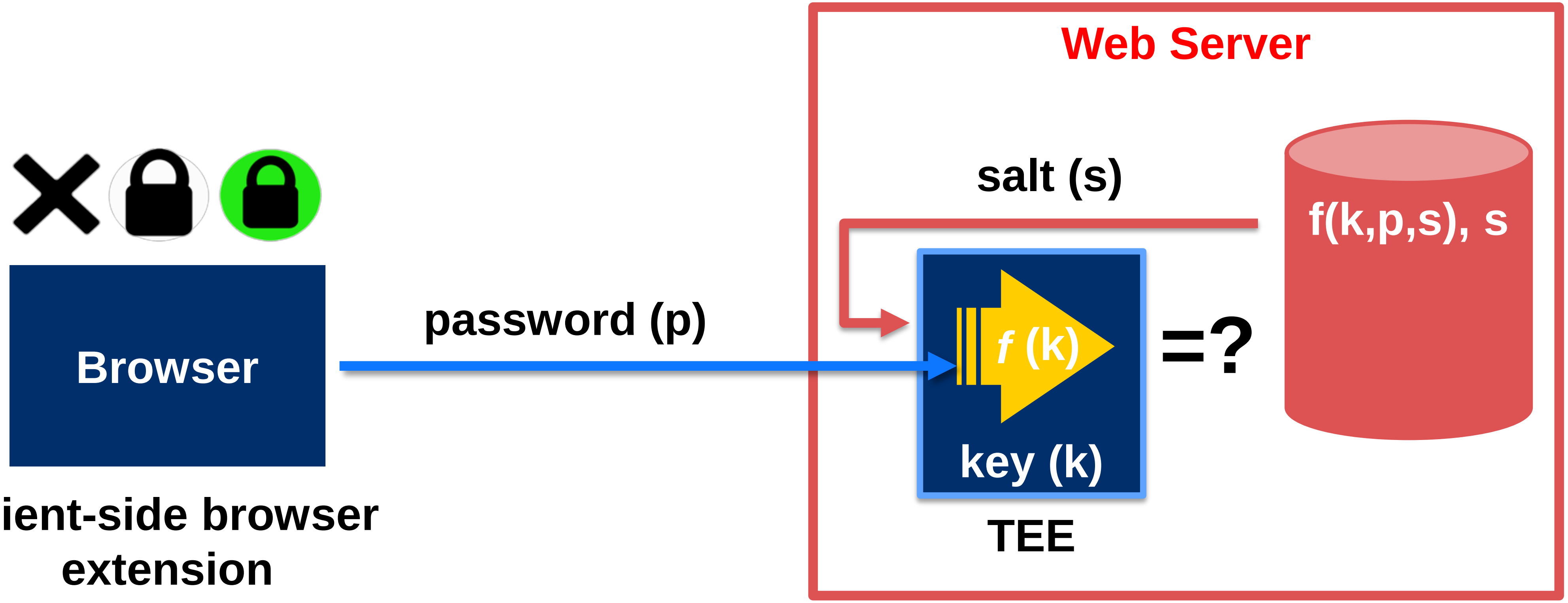
- **Example: protecting password-based web authentication systems**

Novel platform security mechanisms

- **Examples:**
  - Linux kernel hardening
  - Hardening embedded systems (C-Flat and HardScope)

SafeKeeper: Protecting Web Passwords

How can we use widely available trusted hardware to deter password database theft and server compromise?



Client-side browser extension

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

SAFE KEEPER

Linux kernel hardening

What vulnerabilities exist in the Linux kernel? How to mitigate them?

Randomization can’t stop BPF JIT spray

https://www.blackhat.com/eu-16/briefings.html# randomization-cant-stop-bpf-jit-spray

Preventing reference counter overflows and pointer bound violations

https://ssg.aalto.fi/projects/kernel-hardening/

Runtime Attacks

Run-time attacks still a major threat for PCs, mobile and embedded devices

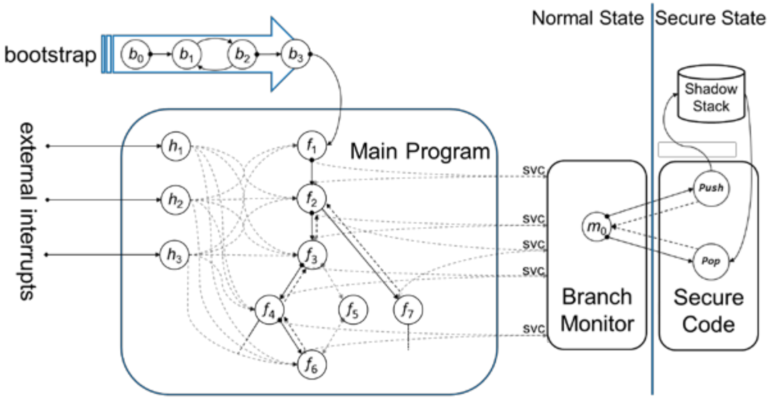
Software written in memory unsafe languages such as C/C++

- Suffer from various memory-related errors

Memory errors may allow run-time attacks to compromise program behaviour

- *Control-flow hijacking / code injection*
- *Return-Oriented Programming* (ROP)
- *Non-control-data attacks*
- *Data-Oriented Programming* (DOP)

Hardening Embedded Systems



CaRE architecture overview

C-FLAT

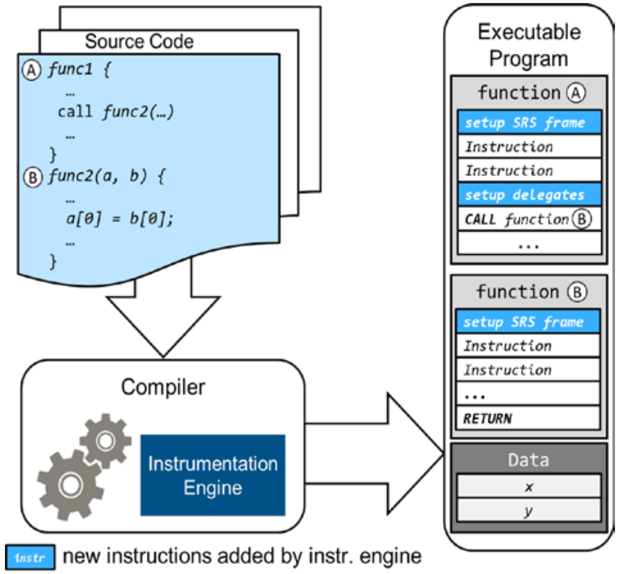
- Control-flow attestation for embedded devices

CFI CaRe

- Hardware-supported call and return enforcement on TrustZone-M

HardScope

- Thwarting DOP attacks with hardware-enforced scoping



https://ssg.aalto.fi/projects/embedded-systems-security/

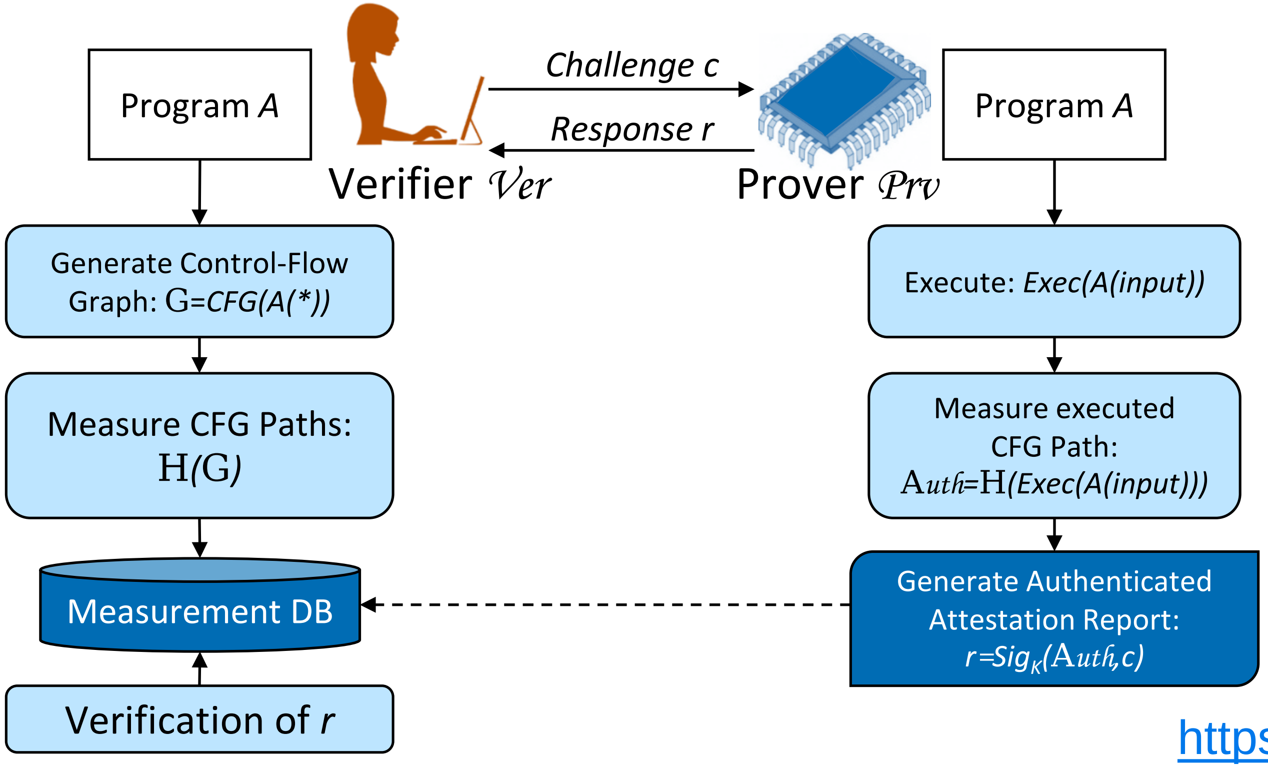
Control-Flow Attestation

How can a trusted verifier learn about run-time attacks and dynamic behavior of an embedded device?

- Current *remote attestation* schemes measure only integrity of program binary
- Control-flow and data-oriented attacks corrupt runtime state of program

C-FLAT: Attestation for Run-time Behavior (high-level idea)

Trace and record control flow of prover and aggregate measurement in *hash-chain*


Program *A*
Challenge *c*
Response *r*
Verifier *Ver*
Prover *Prv*
Program *A*
Generate Control-Flow Graph: G=*CFG(A(*))*
Execute: *Exec(A(input))*
Measure CFG Paths: H*(*G*)*
Measure executed CFG Path: Auth=H*(Exec(A(input)))*
Measurement DB
Generate Authenticated Attestation Report: *r=Sig$_K$(*Auth*,c)*
Verification of *r*

https://arxiv.org/abs/1605.07763

Aalto University
TECHNISCHE UNIVERSITÄT DARMSTADT
UCI
intel
Collaborative Research Institute for Secure Computing
TRUSTONIC

Run-time Scope Enforcement (high-level idea)

Reduce effects of attacks that corrupt data by
enforcing variable visibility rules at run time

Challenges:

- *Lexical scope* of variables used only in static checks by compiler
  → **scope information not typically available at run time**
- *Granularity* of enforcement, module-level fault isolation not sufficient
  → **subjects functions, objects typed data in memory**
- *Context sensitive access*, distinct function invocations must operate with different rules
  → **pointers may be legitimately passed down (and up) call chain**
- *Pervasiveness*, ability to mediate all memory accesses
  → **enforcement must the efficient**

HardScope: Hardware-assisted Run-Time Scope Enforcement

Generic architectural extension enabling hardware-assisted run-time scope enforcement

HardScope consists of:

- Hardware-component for managing run-time access rules
- 6 new instructions configure HardScope-hardware with access rules
- Rule-enforcement added to `load` / `store`
- Compiler-extension that instruments software to use HardScope hardware

Enables flexible adjustment of enforcement granularity at instrumentation time

- Module-level → Function-level → Block-level (e.g. for-loop, if-else-statement block)

Implementation

Prototype on *PULPino* SoC on *ZedBoard* FPGA

- Instruction set extension integrated into open-source RISC-V processor

Toolchain support:

- Automatic instrumentation via compiler plug-in integrated into RISC-V GCC toolchain
- Software simulation of RSE-enabled RISC-V processor integrated into Spike simulator

Minimal performance impact on CoreMark embedded benchmark

- Incurs only ~3% overhead

https://arxiv.org/abs/1705.10295

Aalto University

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Research: ML & Security

Machine learning and Security

Machine learning for security and privacy

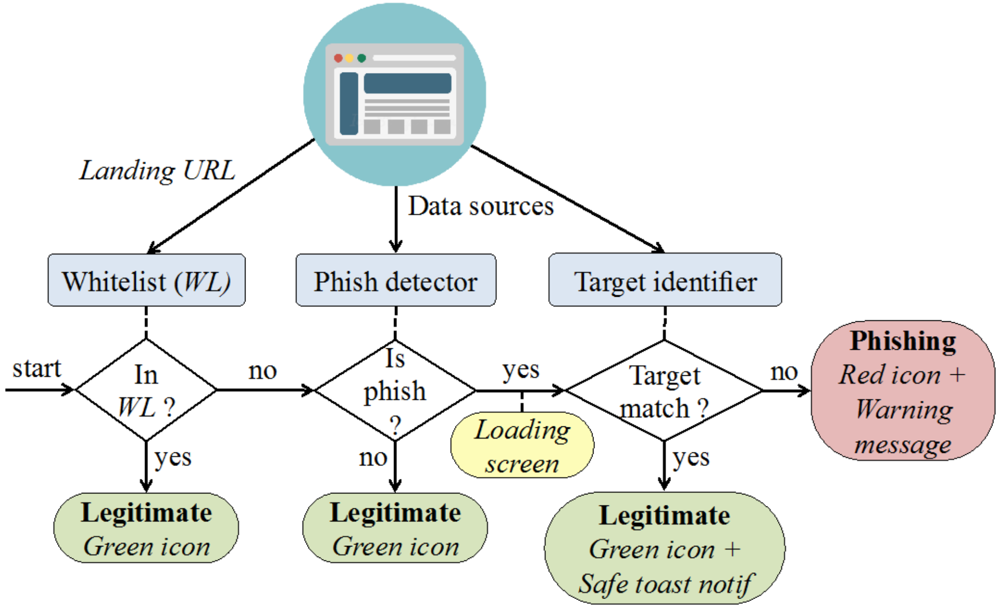
- **Examples:**
  - Fast client-side phishing detection (off-the-hook)
  - Detection of vulnerable/compromised IoT devices (IoT Sentinel and DÏoT

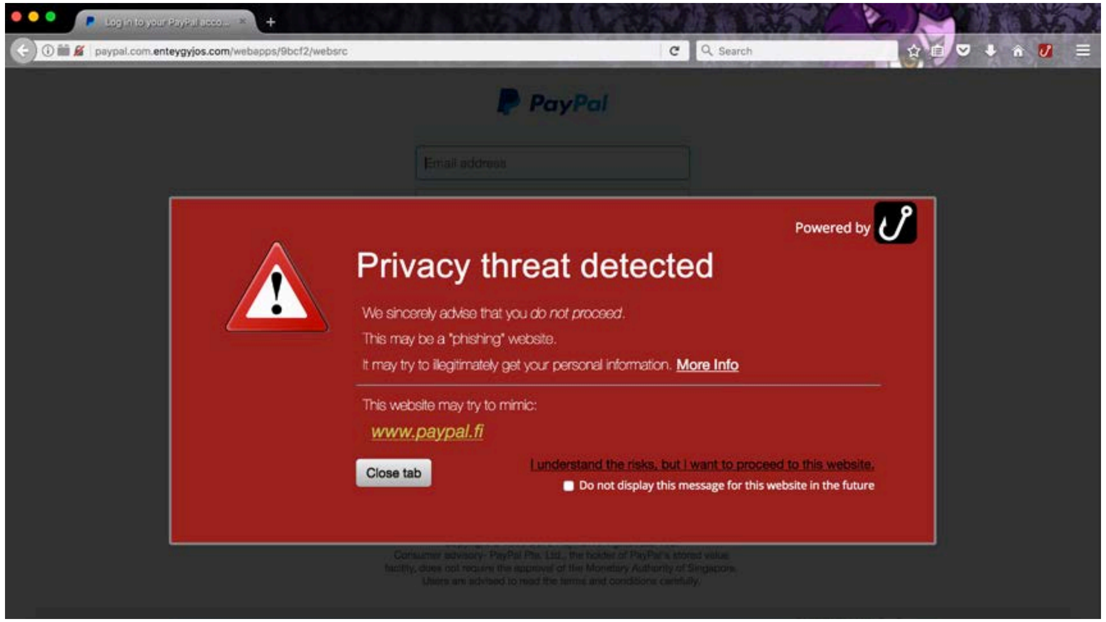
Security and privacy of machine-learning based systems

- **Examples:**
  - Privacy-preserving neural network predictions (MiniONN)
  - Model stealing: attacks and defenses

Fast client-side Phishing Protection

How to improve phish detection by modeling constraints on phishers?




Log in to your PayPal acco...
paypal.com.enteygyjos.com/webapps/9bcf2/websrc
Search
PayPal
Email address
Powered by

Privacy threat detected

We sincerely advise that you *do not proceed.*

This may be a "phishing" website.

It may try to illegitimately get your personal information. **More Info**

This website may try to mimic:

www.paypal.fi

Close tab

I understand the risks, but I want to proceed to this website.

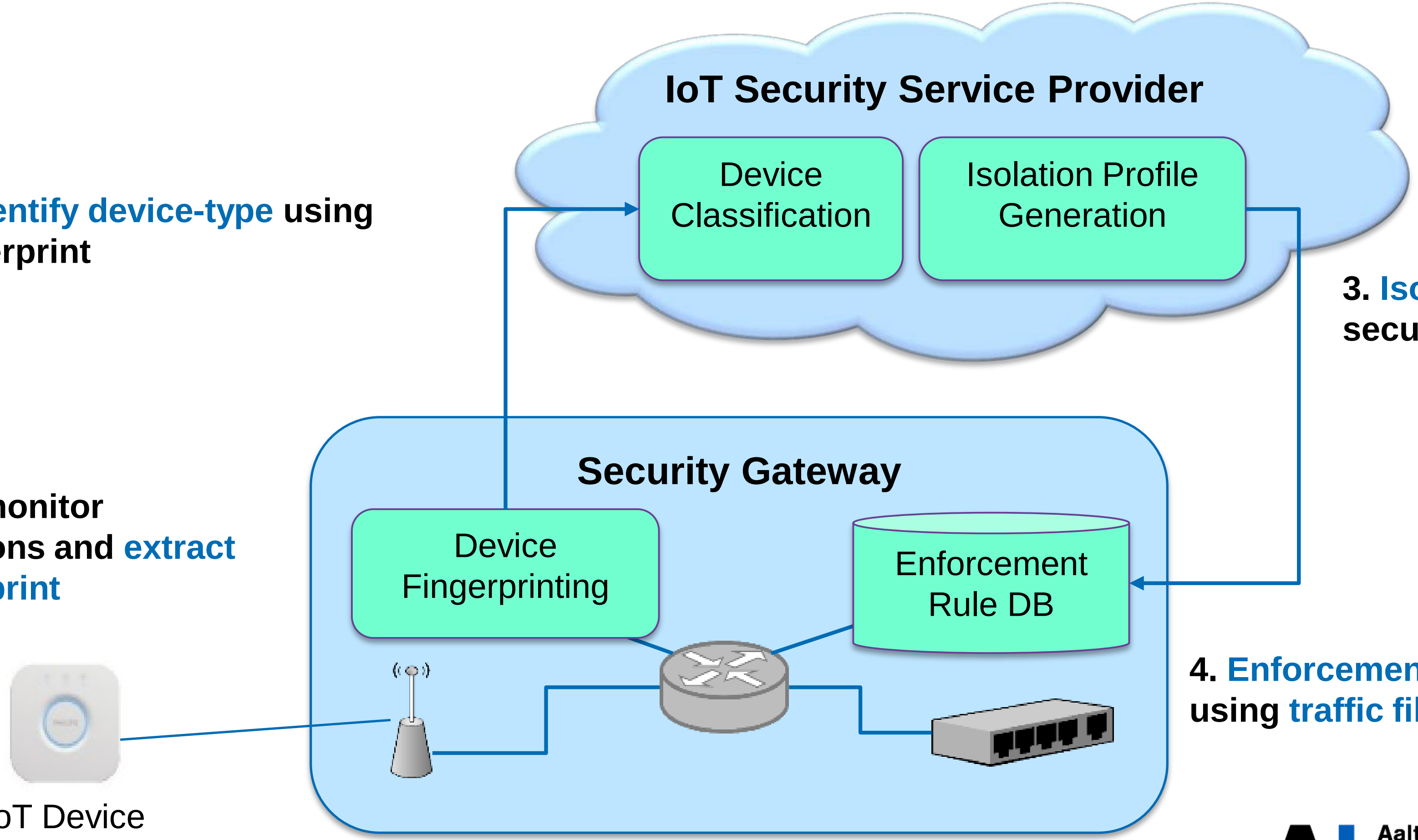
□ Do not display this message for this website in the future

Consumer advisory- PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

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

IoT Sentinel: Automated device-type identification

How to protect smart home networks from vulnerable IoT devices?



1. Passively monitor communications and **extract device fingerprint**

2. **Identify device-type** using fingerprint

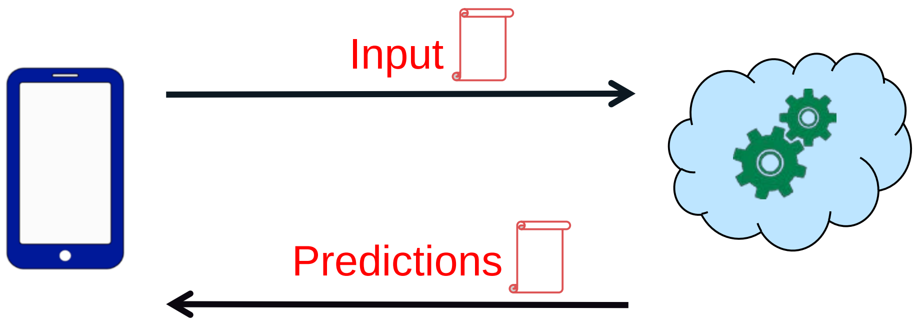
3. **Isolation decision** based on security assessment of device-type

4. **Enforcement** of device isolation using **traffic filtering**

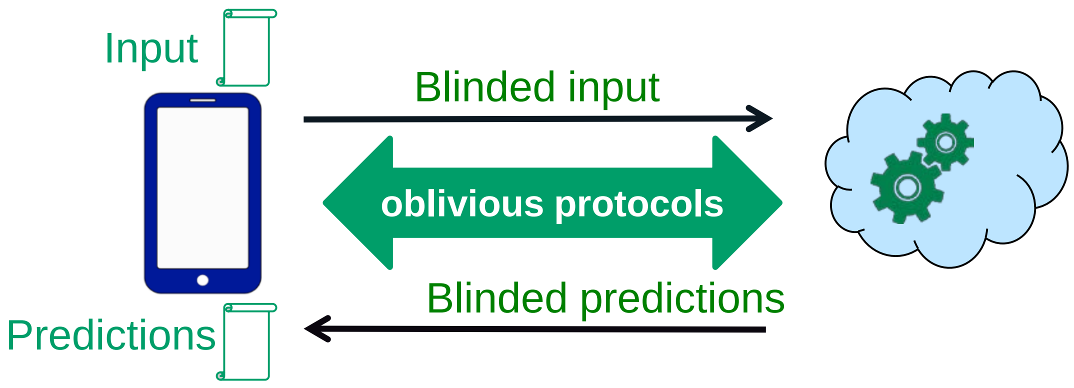
https://ssg.aalto.fi/projects/seliot

Privacy-preserving Neural Networks

How to make cloud-based prediction models preserve privacy?



violates clients’ privacy



Use inexpensive cryptographic tools

MiniONN (ACM CCS 2017)

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

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

Research: Other

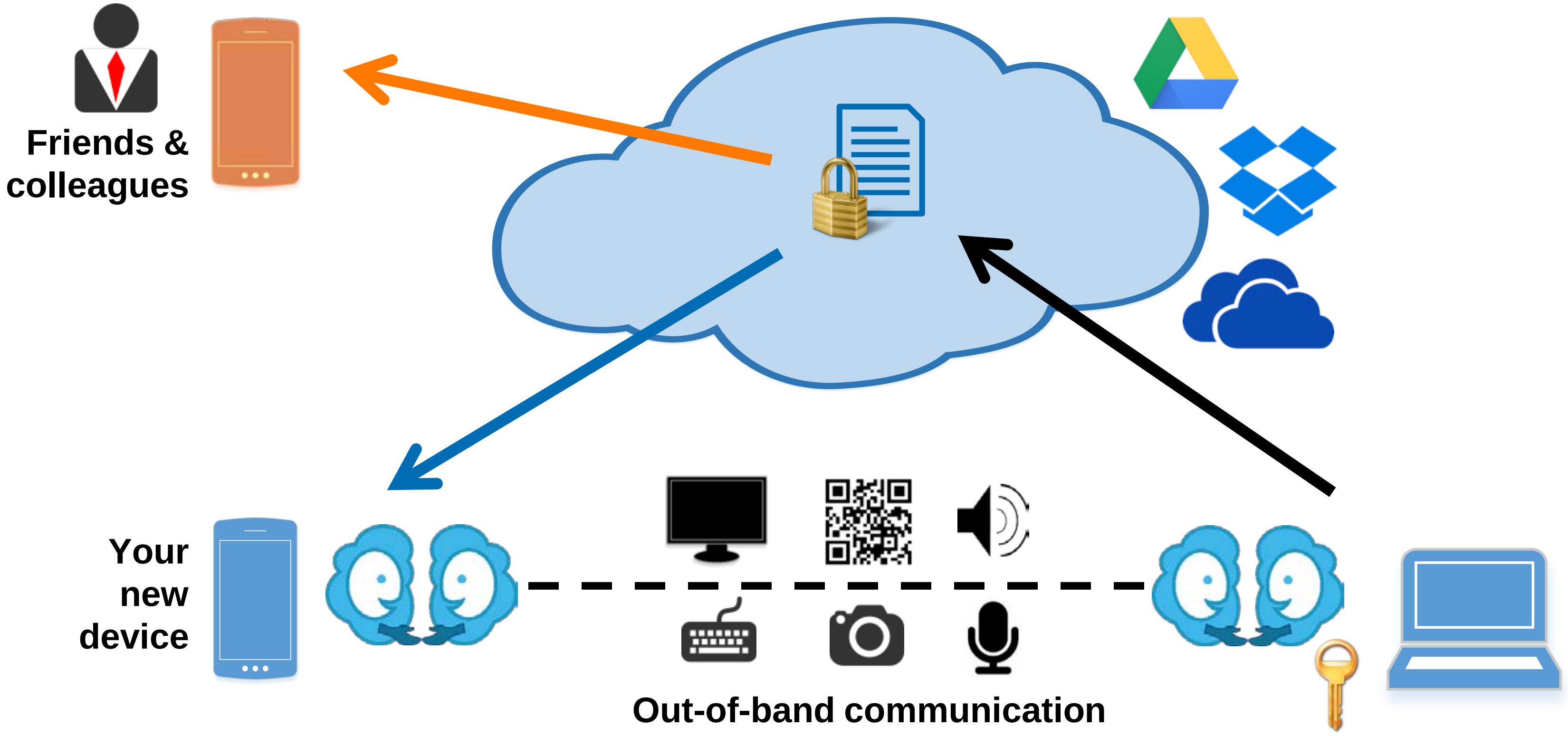
Building systems that are secure, usable, and deployable

Skip to Education

Skip to summary

OmniShare: Secure Cloud Storage

How can you share your data securely
with anyone you like, anywhere you like?



TECHNISCHE UNIVERSITÄT DARMSTADT

ACADEMY OF FINLAND

intel Collaborative Research Institute for Secure Computing

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

Current themes: Emerging topics

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

- Can hardware security mechanisms help design scalable consensus schemes?

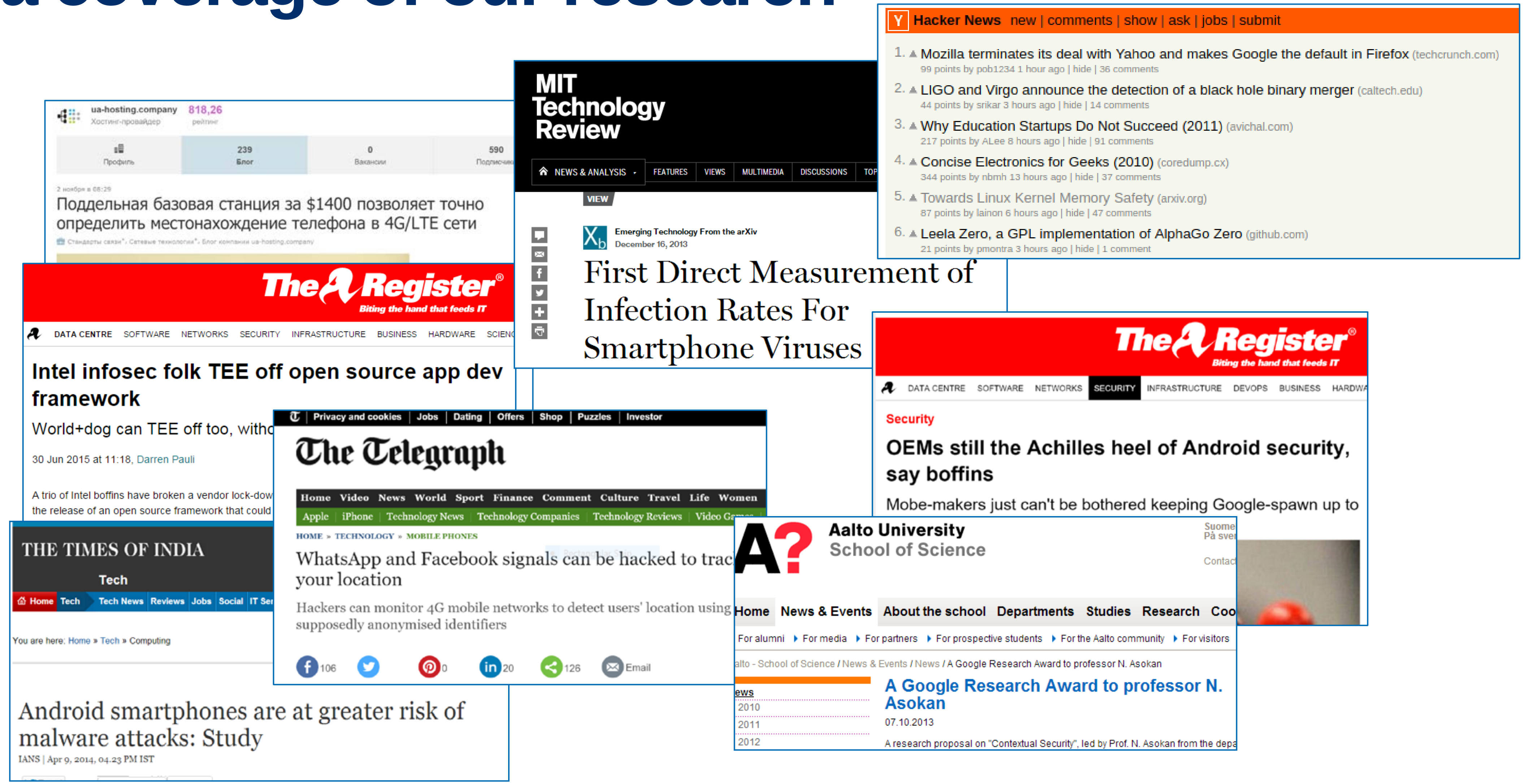
Securing IoT (scalability, usability) [AoF SELIoT]

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

Stylometry and security [HICT scholarship]

- Can text analysis help detect deception?

Media coverage of our research



ua-hosting.company 818,26
Хостинг-провайдер рейтинг

Профиль | 239 Блог | 0 Вакансии | 590 Подписчики

2 ноября в 08:29

Поддельная базовая станция за $1400 позволяет точно определить местонахождение телефона в 4G/LTE сети

Стандарты связи*, Сетевые технологии*, Блог компании ua-hosting.company

Y Hacker News new | comments | show | ask | jobs | submit

1. ▲ Mozilla terminates its deal with Yahoo and makes Google the default in Firefox (techcrunch.com)
   99 points by pob1234 1 hour ago | hide | 36 comments
2. ▲ LIGO and Virgo announce the detection of a black hole binary merger (caltech.edu)
   44 points by srikar 3 hours ago | hide | 14 comments
3. ▲ Why Education Startups Do Not Succeed (2011) (avichal.com)
   217 points by ALee 8 hours ago | hide | 91 comments
4. ▲ Concise Electronics for Geeks (2010) (coredump.cx)
   344 points by nbmh 13 hours ago | hide | 37 comments
5. ▲ Towards Linux Kernel Memory Safety (arxiv.org)
   87 points by lainon 6 hours ago | hide | 47 comments
6. ▲ Leela Zero, a GPL implementation of AlphaGo Zero (github.com)
   21 points by pmontra 3 hours ago | hide | 1 comment

MIT Technology Review

NEWS & ANALYSIS | FEATURES | VIEWS | MULTIMEDIA | DISCUSSIONS | TOP

VIEW

Emerging Technology From the arXiv
December 16, 2013

First Direct Measurement of Infection Rates For Smartphone Viruses

The Register® Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENC

Intel infosec folk TEE off open source app dev framework

World+dog can TEE off too, witho

30 Jun 2015 at 11:18, Darren Pauli

A trio of Intel boffins have broken a vendor lock-dow
the release of an open source framework that could

Privacy and cookies | Jobs | Dating | Offers | Shop | Puzzles | Investor

The Telegraph

Home Video News World Sport Finance Comment Culture Travel Life Women

Apple | iPhone | Technology News | Technology Companies | Technology Reviews | Video Games

HOME » TECHNOLOGY » MOBILE PHONES

WhatsApp and Facebook signals can be hacked to trac your location

Hackers can monitor 4G mobile networks to detect users' location using supposedly anonymised identifiers

106 0 20 126 Email

The Register® Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWA

Security

OEMs still the Achilles heel of Android security, say boffins

Mobe-makers just can't be bothered keeping Google-spawn up to

THE TIMES OF INDIA

Tech

Home Tech Tech News Reviews Jobs Social IT Ser

You are here: Home » Tech » Computing

Android smartphones are at greater risk of malware attacks: Study

IANS | Apr 9, 2014, 04.23 PM IST

Aalto University
School of Science

Suome
På sver
Contac

Home News & Events About the school Departments Studies Research Coo

For alumni ▸ For media ▸ For partners ▸ For prospective students ▸ For the Aalto community ▸ For visitors

alto - School of Science / News & Events / News / A Google Research Award to professor N. Asokan

ews
2010
2011
2012

A Google Research Award to professor N. Asokan

07.10.2013

A research proposal on "Contextual Security", led by Prof. N. Asokan from the depa

Research Funding (Summary)

Cloud Security Services (CloSer 2016 - 2018)

- Funded by Business Finland (formerly Tekes)

Securing Lifecycles of IoT devices (SELIoT 2017 - 2019)

- Funded by NSF and Academy of Finland (WiFiUS program)
- Aalto (Asokan), UC Irvine (Tsudik), U Florida (Traynor)

Intel Collaborative Research Institute (ICRI-SC 2014 – 2017 & ICRI-CARS 2017 - 2020)

- Secure Computing
- Collaborative, Autonomous and Resilient Systems

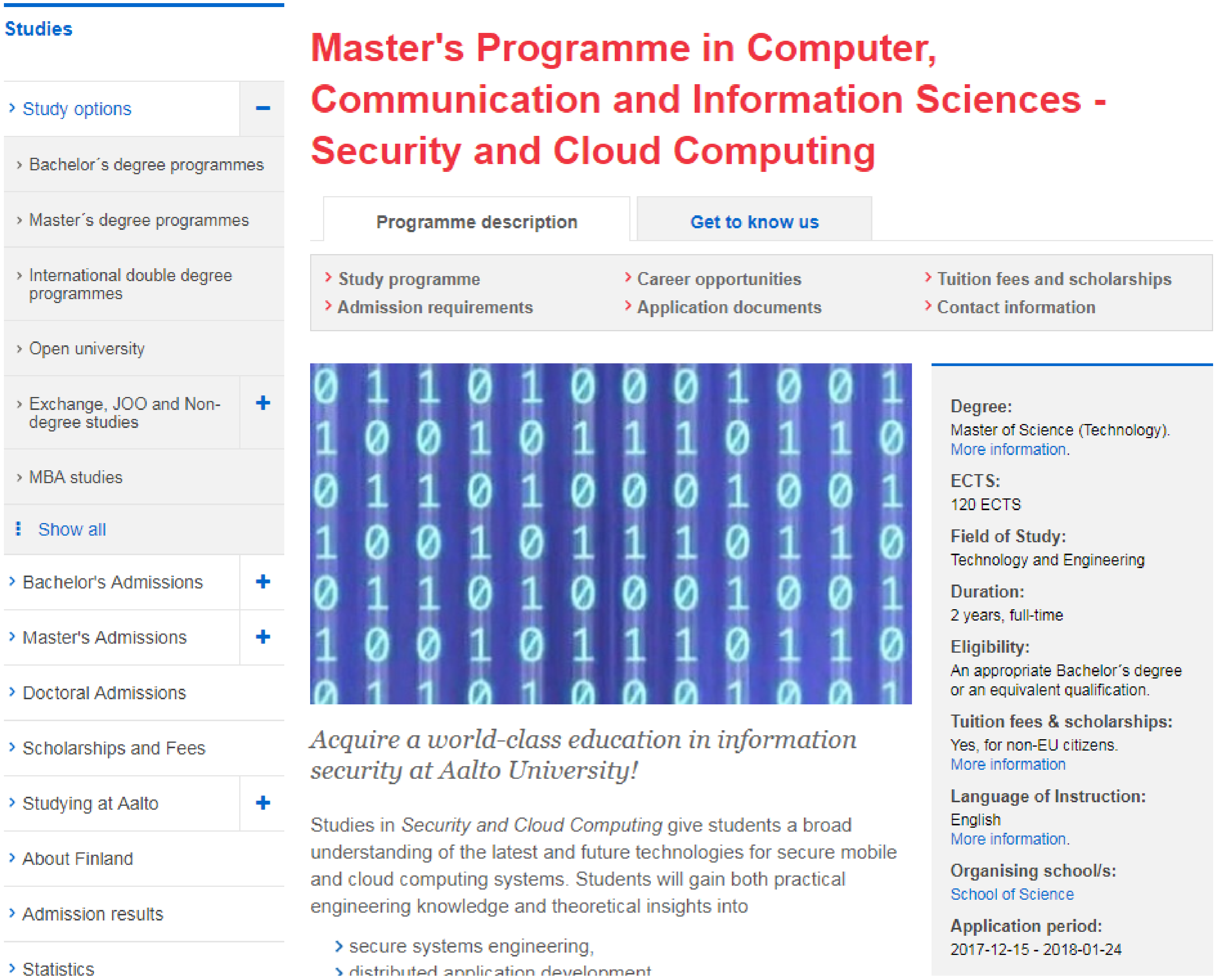
Blockchain Consensus and Beyond (Bcon 2017 - 2020)

- Funded by Academy of Finland

Education

Training the next generation of information security researchers and professionals

Skip to summary



Studies

- Study options −
  - Bachelor´s degree programmes
  - Master´s degree programmes
  - International double degree programmes
  - Open university
  - Exchange, JOO and Non-degree studies +
  - MBA studies
  - Show all
- Bachelor's Admissions +
- Master's Admissions +
- Doctoral Admissions
- Scholarships and Fees
- Studying at Aalto +
- About Finland
- Admission results
- Statistics

Master's Programme in Computer, Communication and Information Sciences - Security and Cloud Computing

Programme description | Get to know us

- Study programme
- Admission requirements
- Career opportunities
- Application documents
- Tuition fees and scholarships
- Contact information

Acquire a world-class education in information security at Aalto University!

Studies in *Security and Cloud Computing* give students a broad understanding of the latest and future technologies for secure mobile and cloud computing systems. Students will gain both practical engineering knowledge and theoretical insights into

- secure systems engineering,
- distributed application development

Degree:
Master of Science (Technology). More information.

ECTS:
120 ECTS

Field of Study:
Technology and Engineering

Duration:
2 years, full-time

Eligibility:
An appropriate Bachelor´s degree or an equivalent qualification.

Tuition fees & scholarships:
Yes, for non-EU citizens.
More information

Language of Instruction:
English
More information.

Organising school/s:
School of Science

Application period:
2017-12-15 - 2018-01-24

http://www.aalto.fi/en/studies/education/programme/security_and_cloud_computing/

SECCLO

Master's Programme in Security and Cloud Computing

(Erasmus Mundus)

Applications: 4.12.2017 – 17.01.2018

Scholarships available

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

A! 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

Helsinki-Aalto Center for Information Security (HAIC)

Joint initiative: Aalto University and University of Helsinki https://haic.aalto.fi/

Mission: attract/train top students in information security

- Offers financial aid to top students in both CCIS Security and Cloud Computing & SECCLO
- Three scholars in 2017; Up to five (expected) in 2018

Call for donors and supporters

- Supported by donations from F-Secure, Intel, Nixu, Huawei, and Aalto University School of Science

2018

2017

InfoSec Research and Education @ Aalto

20+ MSc and BSc theses yearly

2014

- Runner-up: Best CS MSc Thesis in Finland
- WWW (1)
- ACM ASIACCS (1)
- Proc. IEEE (1)
- Best InfoSec MSc thesis in Finland
- PerCom (1)
- ACM CCS (1)
- Black Hat USA (1)

2015

- ACM WiSec (1)
- PerCom (1)
- ACM CCS (2)
- Black Hat Europe (1)
- UbiComp (1)
- ACM ASIACCS (1)

2016

- ACM CCS (1)
- NDSS (2)
- IEEE ICDCS (1)
- Best InfoSec MSc thesis in Finland
- CeBIT (1)
- Black Hat Europe (1)

2017

- ACM ASIACCS (1)
- DAC (1)
- IEEE ICDCS (2)
- IEEE SECON (1)
- Best InfoSec MSc thesis in Finland
- ACM CCS (1)
- IEEE IC (1)
- RAID (1)
- IEEE TC (1)

2018

- WWW (1)
- IEEE Euro S&P (1)
- CT-RSA (1)
- IEEE DSN (1)

(awards in green)

https://ssg.aalto.fi/about-us/

Information Security Research and Education at Aalto

N. Asokan

http://asokan.org/asokan/

@nasokan