Aalto University

Information Security Research and Education

N. Asokan
Twitter: @nasokan, WWW: https://asokan.org/asokan

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

Previously

Nokia (14 y; built up Nokia security research team)
IBM Research (3 y)

More information on the web (https://asokan.org/asokan) or Twitter (@nasokan)

Secure Systems Group

Prof N. Asokan

Professor, Department of Computer Science

Director: Helsinki-Aalto Center for Information Security

https://asokan.org/asokan/

Prof Tuomas Aura

Professor, Department of Computer Science

https://people.aalto.fi/tuomas_aura

Dr Andrew Paverd

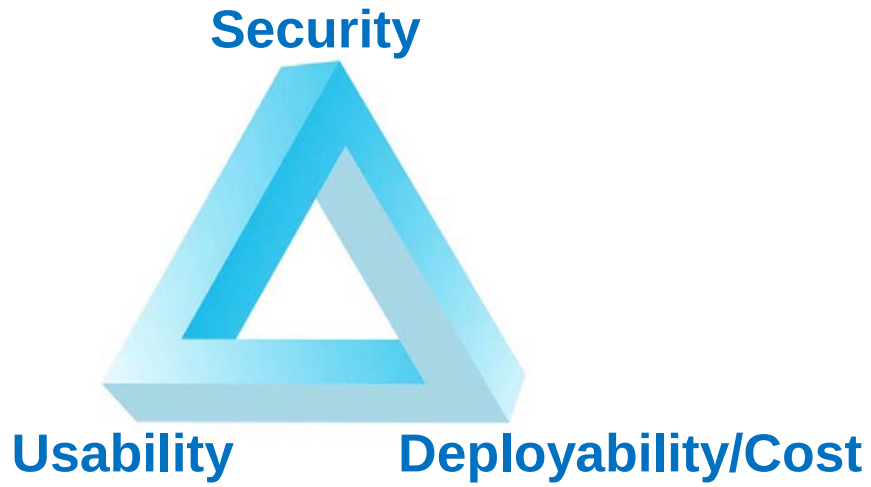
Research Fellow, Department of Computer Science

Deputy Director: Helsinki-Aalto Center for Information Security

https://ajpaverd.org

Secure Systems Group: 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/

In Asokan's projects:

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

Several MSc students

- Best InfoSec thesis in Finland 2017, 2016 & 2014, 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, Huawei]

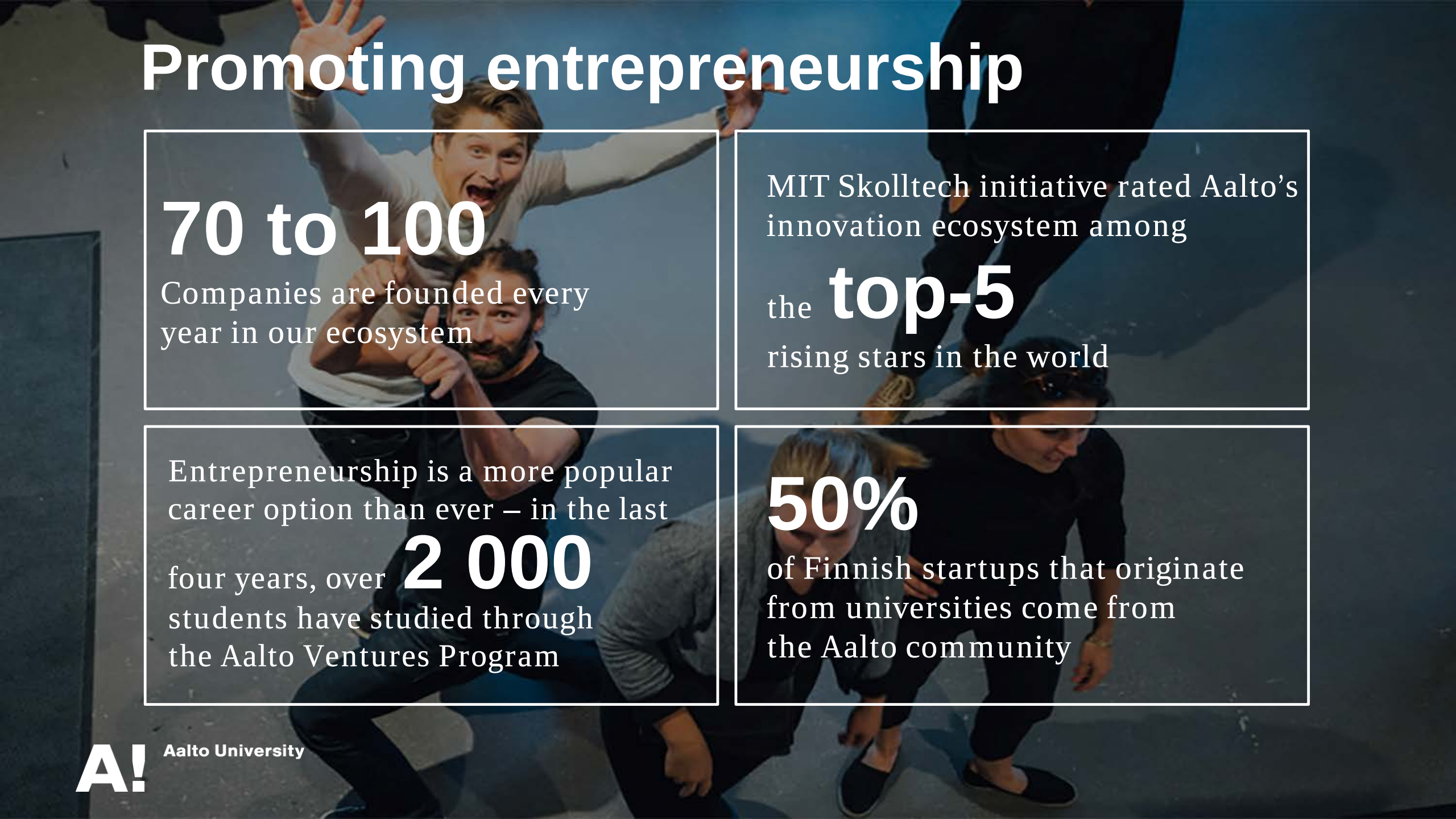
Aalto University

Established in 2010, named in honour of ***Alvar Aalto***, the famous Finnish architect.

Science and art meet technology and business.

Aalto University

Promoting entrepreneurship



70 to 100

Companies are founded every year in our ecosystem

MIT Skolltech initiative rated Aalto's innovation ecosystem among the **top-5** rising stars in the world

Entrepreneurship is a more popular career option than ever – in the last four years, over **2 000** students have studied through the Aalto Ventures Program

50%

of Finnish startups that originate from universities come from the Aalto community

Aalto University


SLUSH
NOBODY IN THEIR RIGHT MIND WOULD COME TO HELSINKI IN NOVEMBER.
http://www.slush.org/

Research

Building systems that are secure, usable, and deployable

Current themes: Platform Security

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

HardScope: Thwarting DOP with Hardware-assisted Run-time Scope Enforcement

Thomas Nyman, Ghada Dessouky, Shaza Zeitouni, Aaro Lehikoinen, Andrew Paverd, N. Asokan, Ahmad-Reza Sadeghi

(Submitted on 29 May 2017)

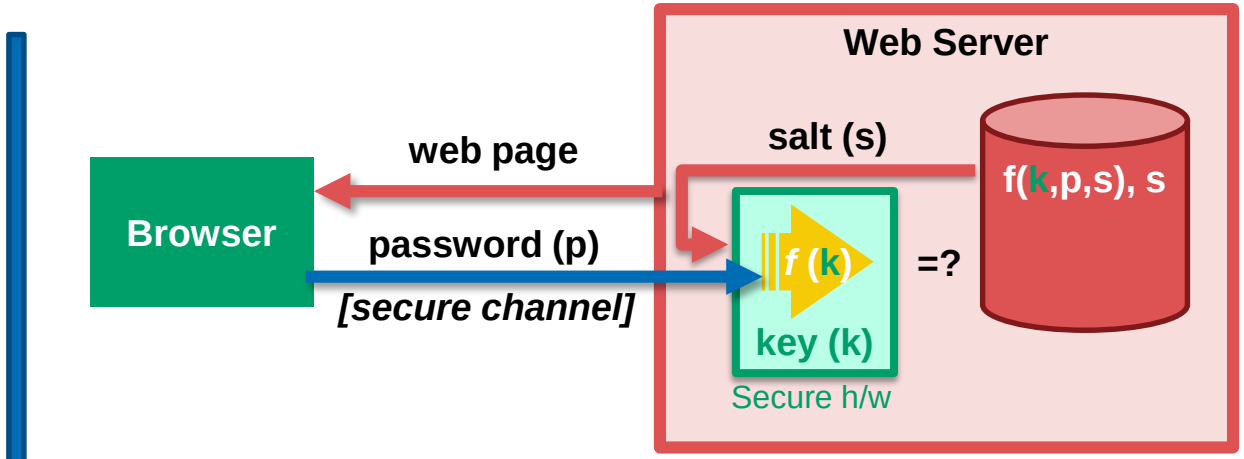
The widespread use of memory unsafe programming languages (e.g., C and C++), especially in embedded systems and the Internet of Things (IoT), leaves many systems vulnerable to memory corruption attacks. A variety of defenses have been proposed to mitigate attacks that exploit memory errors to hijack the control flow of the code at run-time, e.g., (fine-grained) ASLR or Control Flow Integrity (CFI). However, recent work on data-oriented programming (DOP) demonstrated the possibility to construct highly-expressive (Turing-complete) attacks, even in the presence of these state-of-the-art defenses. Although multiple real-world DOP attacks have been demonstrated, no suitable defenses are yet available.
We present run-time scope enforcement (RSE), a novel approach designed to mitigate all currently known DOP attacks by enforcing compile-time memory safety constraints (e.g., variable visibility rules) at run-time. We also present HardScope, a proof-of-concept implementation of hardware-assisted RSE for the new RISC-V open instruction set architecture. We demonstrate that HardScope mitigates all currently known DOP attacks at multiple points in each attack. We have implemented HardScope in hardware on the open-source RISC-V Pulpino microcontroller. Our cycle-accurate simulation shows a real-world performance overhead of 7.1% when providing complete mediation of all memory accesses.

https://arxiv.org/abs/1705.10295

Current themes: Platform Security

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

Example: SafeKeeper – using Intel SGX on server-side to protect passwords

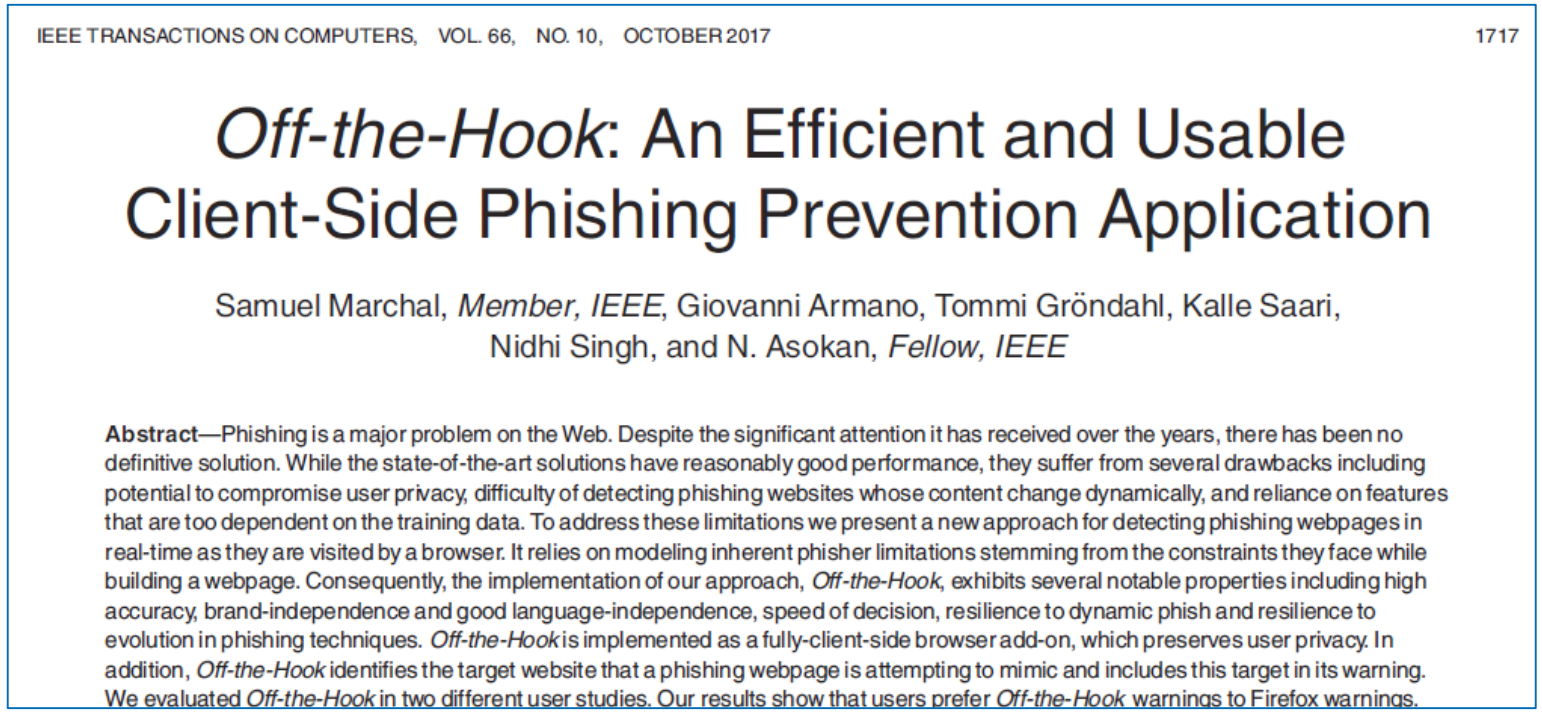


Use secure hardware on server side

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

SAFE KEEPER

Current themes: Machine Learning & Security



IEEE TRANSACTIONS ON COMPUTERS, VOL. 66, NO. 10, OCTOBER 2017

Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application

Samuel Marchal, *Member, IEEE*, Giovanni Armano, Tommi Gröndahl, Kalle Saari, Nidhi Singh, and N. Asokan, *Fellow, IEEE*

Abstract—Phishing is a major problem on the Web. Despite the significant attention it has received over the years, there has been no definitive solution. While the state-of-the-art solutions have reasonably good performance, they suffer from several drawbacks including potential to compromise user privacy, difficulty of detecting phishing websites whose content change dynamically, and reliance on features that are too dependent on the training data. To address these limitations we present a new approach for detecting phishing webpages in real-time as they are visited by a browser. It relies on modeling inherent phisher limitations stemming from the constraints they face while building a webpage. Consequently, the implementation of our approach, *Off-the-Hook*, exhibits several notable properties including high accuracy, brand-independence and good language-independence, speed of decision, resilience to dynamic phish and resilience to evolution in phishing techniques. *Off-the-Hook* is implemented as a fully-client-side browser add-on, which preserves user privacy. In addition, *Off-the-Hook* identifies the target website that a phishing webpage is attempting to mimic and includes this target in its warning. We evaluated *Off-the-Hook* in two different user studies. Our results show that users prefer *Off-the-Hook* warnings to Firefox warnings.

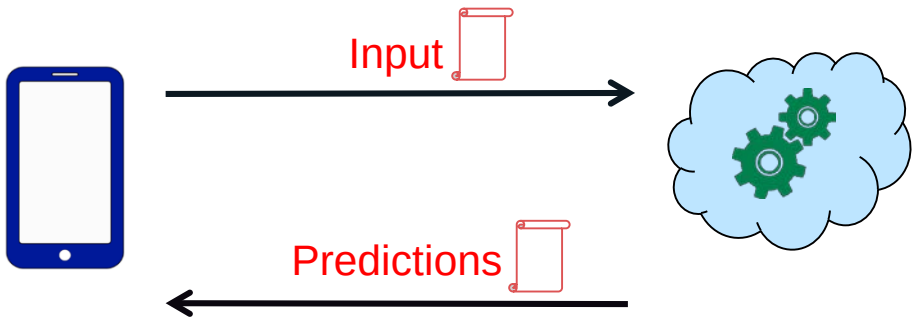
https://ssg.aalto.fi/projects/phishing/

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

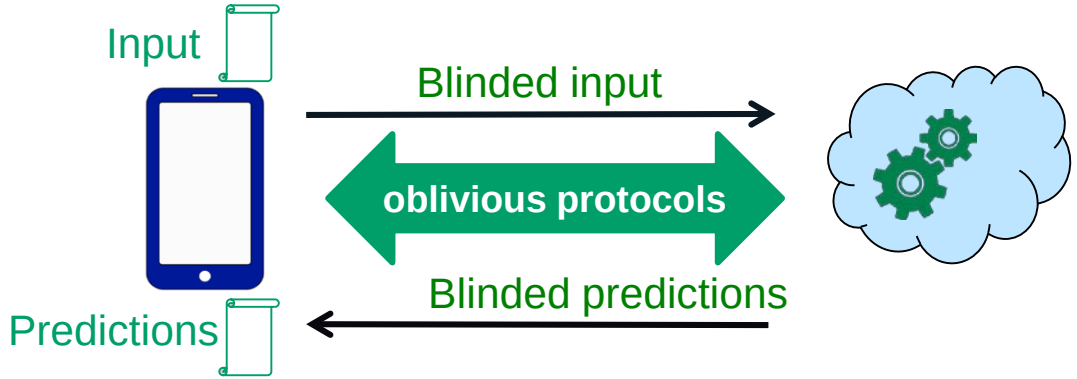
Current themes: Machine Learning & Security

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

Example: MiniONN – privacy-preserving neural network predictions



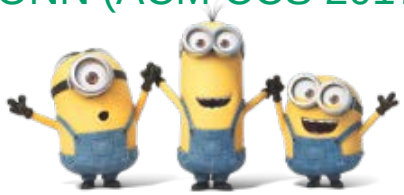
violates clients' privacy



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

intel Collaborative Research Institute for Secure Computing

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

ICRI-SC for mobile and embedded systems security

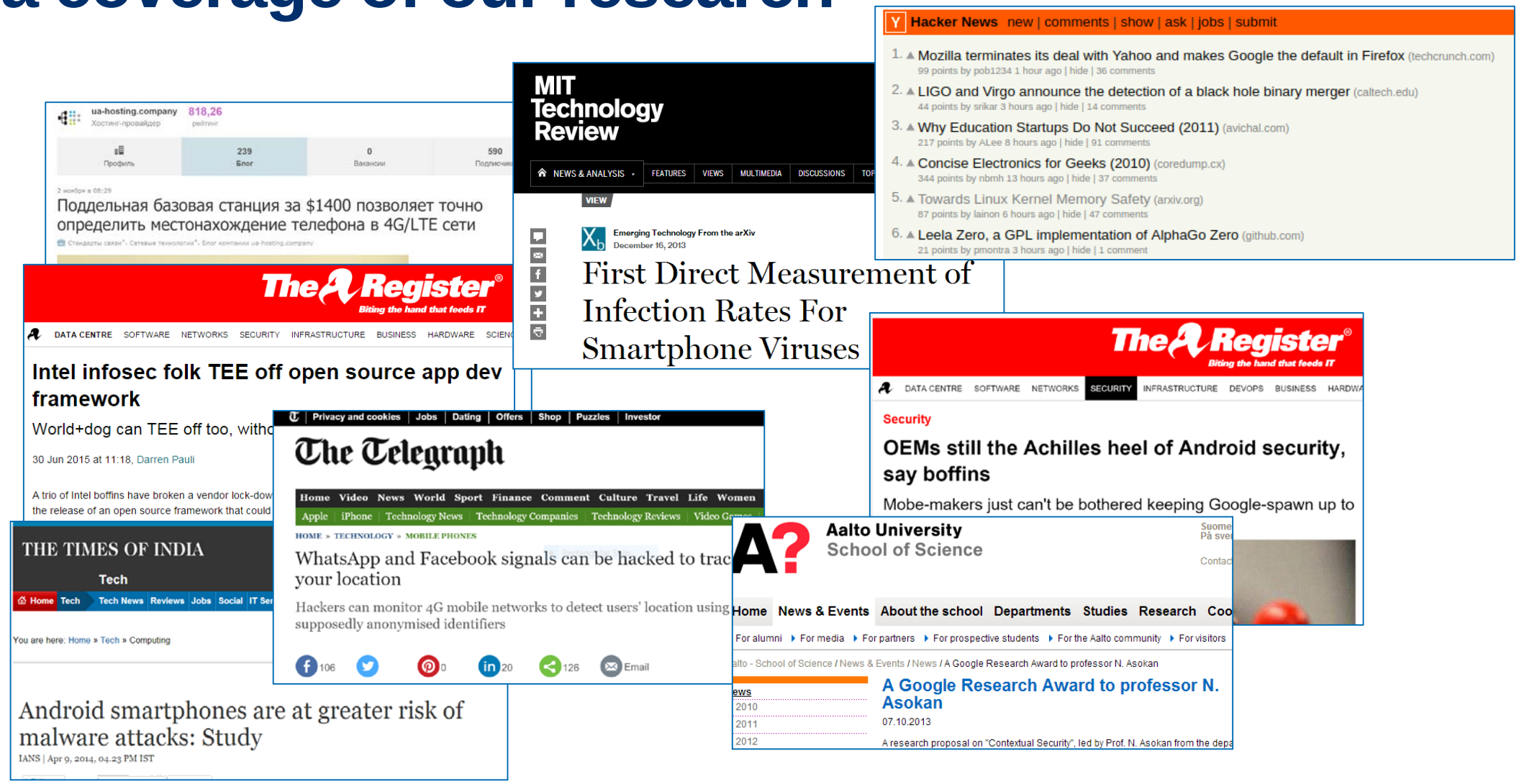
- 2012-2017 (Aalto, TU Darmstadt, UH; Aalto joined in 2014)
- Nearly 1 M€ invested in Aalto and UH

ICRI-CARS for autonomous systems security

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

intel Research Institute for Collaborative Autonomous and Resilient Systems

Media coverage of our research



Education

Training the next generation of information security researchers and professionals

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

~20 scholarships

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 1632 Universitas Tartuensis

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

Mission: attract/train top students in information security

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

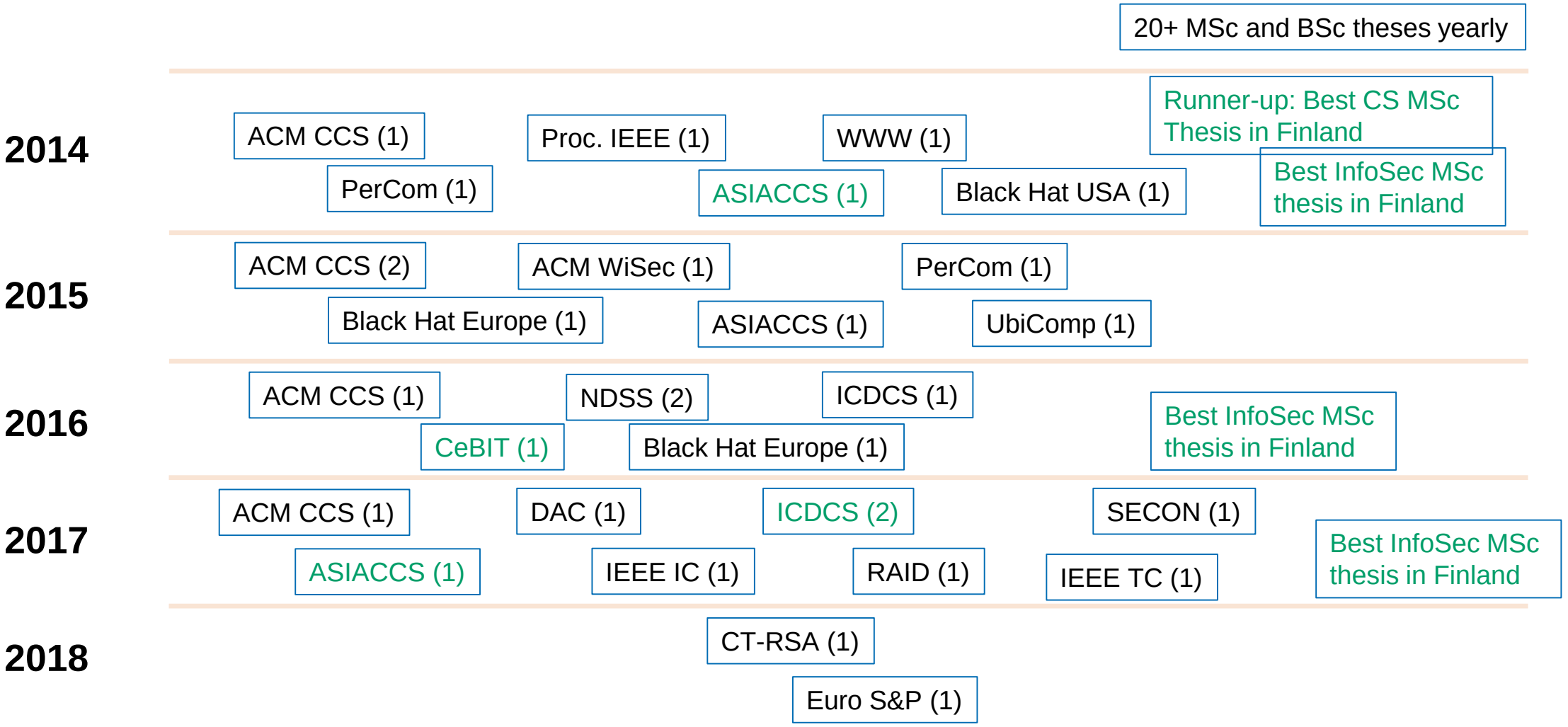
Supported by industry donations

- F-Secure, Intel, Nixu (2017)
- F-Secure, Huawei (2018)

Targeted donations possible

https://haic.aalto.fi/

InfoSec Research and Education @ Aalto



Aalto University

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

Information Security Research and Education

N. Asokan
Twitter: @nasokan, WWW: https://asokan.org/asokan