A!
Aalto University

Systems 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 Fellow (2018)

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 HAIC https://haic.fi

https://asokan.org/asokan/

https://ssg.aalto.fi/

Prof Tuomas Aura

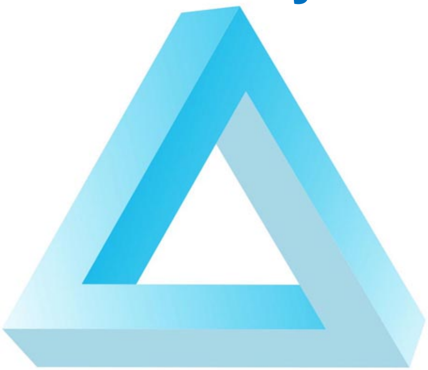
Professor, Department of Computer Science

Director: SECCLO joint degree program https://secclo.eu

https://people.aalto.fi/tuomas_aura

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 ML-based systems even in the presence of adversaries?

Security Protocols

How do we allow devices to communicate securely with one another?

Emerging Topics

E.g., hardware-assisted consensus mechanisms, detecting deception using text analysis

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 ML-based systems even in the presence of adversaries?

Security Protocols

How do we allow devices to communicate securely with one another?

Emerging Topics

E.g., hardware-assisted consensus mechanisms, detecting deception using text analysis

Research: Platform Security

Platform security: overview

Applications of platform security

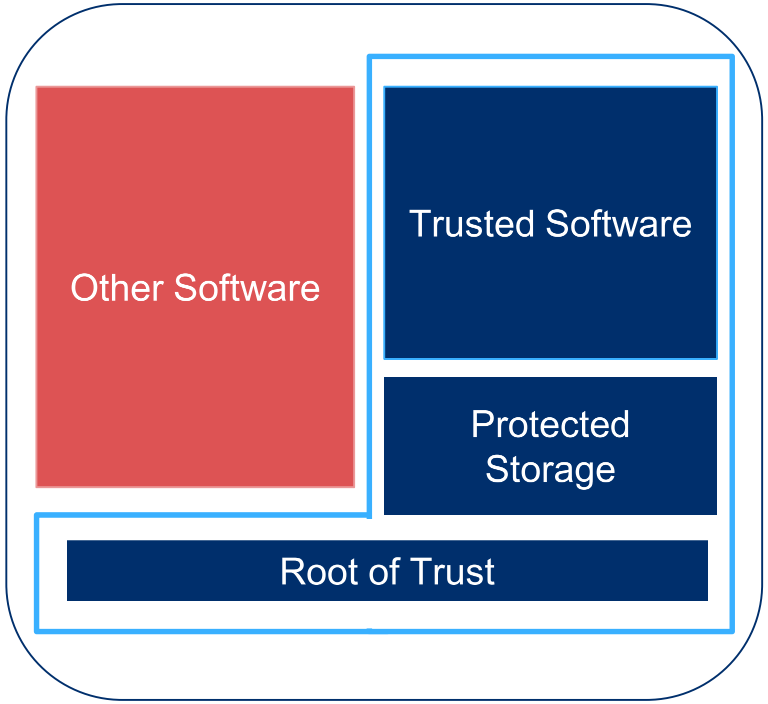
- **Examples**:
  - Protecting password-based web authentication systems (Best Finnish infosec thesis, 2017)
  - Breaking & repairing deniable messaging

Novel platform security mechanisms

- **Examples:**
  - Linux kernel hardening (Best Finnish infosec thesis, 2018)
  - Hardening embedded systems (C-Flat and HardScope)

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

Hardware-security mechanisms are pervasive



Hardware support for

- **Isolated execution: Isolated Execution Environment**
- **Protected storage: Sealing**
- **Ability to report status to a remote verifier: Remote Attestation**

Trusted Execution Environments (TEEs)

Cryptocards

https://www.ibm.com/security/cryptocards/

Trusted Platform Modules

https://www.infineon.com/tpm

ARM TrustZone

https://www.arm.com/products/security-on-arm/trustzone

Intel Software Guard Extensions

https://software.intel.com/en-us/sgx

[A+14] "Mobile Trusted Computing", Proceedings of the IEEE, 102(8) (2014)
[EKA14] "Untapped potential of trusted execution environments", IEEE S&P Magazine, 12:04 (2014)

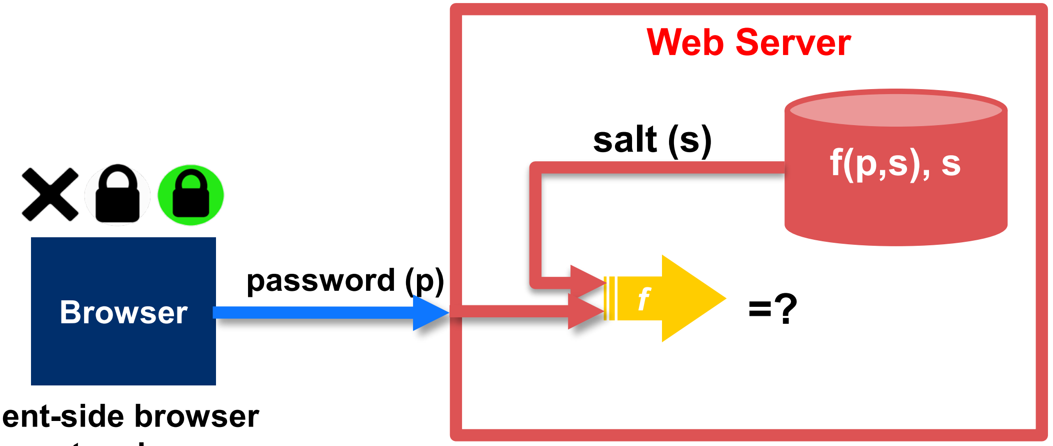
SafeKeeper: Protecting Web Passwords

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

Over 560 Million Passwords Discovered in Anonymous Online Database

Dell Cameron
5/16/17 11:08am · Filed to: YOU'VE BEEN PWNED

19 5



Client-side browser extension

Use secure hardware on server side

SafeKeeper: Protecting Web Passwords

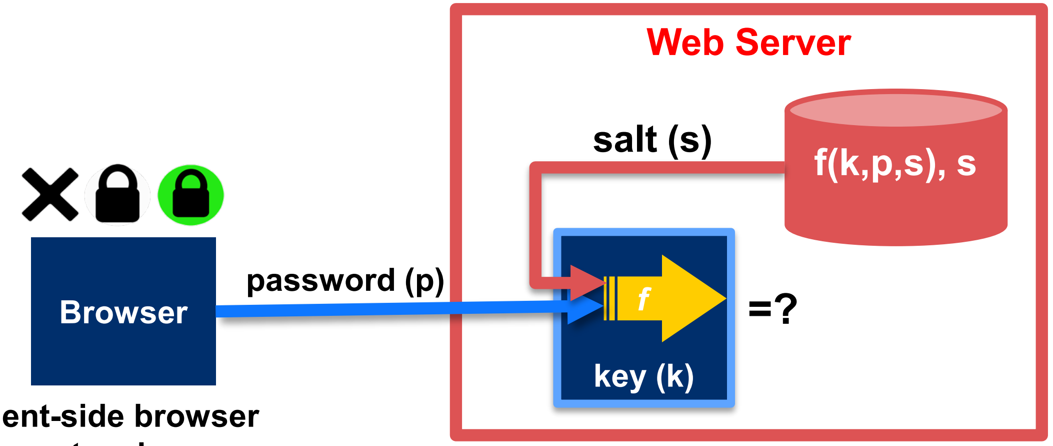
How can we use widely available hardware security mechanisms to deter password database theft and server compromise?

Over 560 Million Passwords Discovered in Anonymous Online Database

Dell Cameron

5/16/17 11:08am · Filed to: YOU'VE BEEN PWNED

19 5



Client-side browser extension

Use secure hardware on server side

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

WebConf 2018 (aka WWW 2018)

SAFE KEEPER

HardScope: Hardware-assisted Run-time Scope Enforcement

How can variable visibility rules be enforced at run-time to prevent run-time attacks?

Run-time attacks violate data integrity

- e.g. data is references known at compile time vs. run-time

Variable visibility rules reduce attacks…

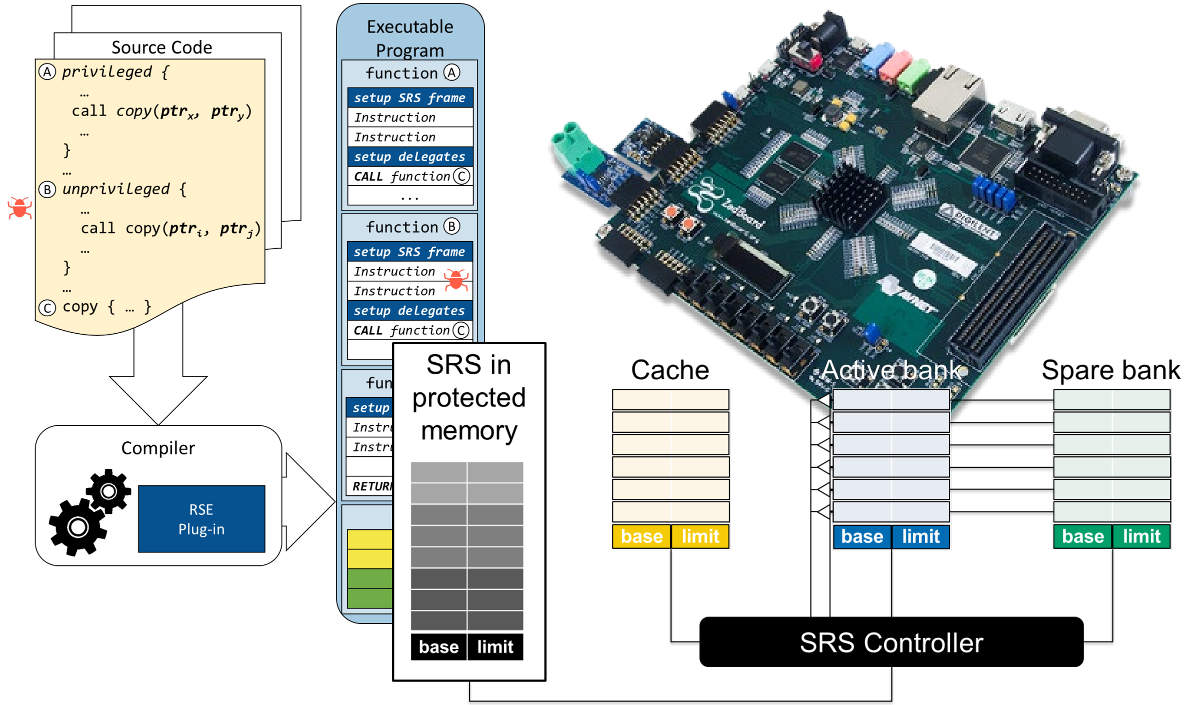
- …but in C/C++ only enforced by compiler

H/W ext. for run-time scope enforcement

- PoC on RISC-V PULPino SoC on FPGA

Low-overhead (~3%) with changes to h/w

- Can apply at different granularities to give resilience against many classes of attacks



Compiler support + Hardware

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

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)

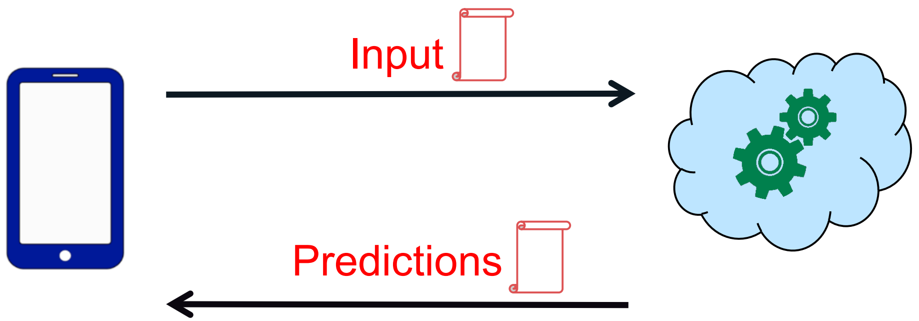
Security and privacy of machine-learning based systems

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

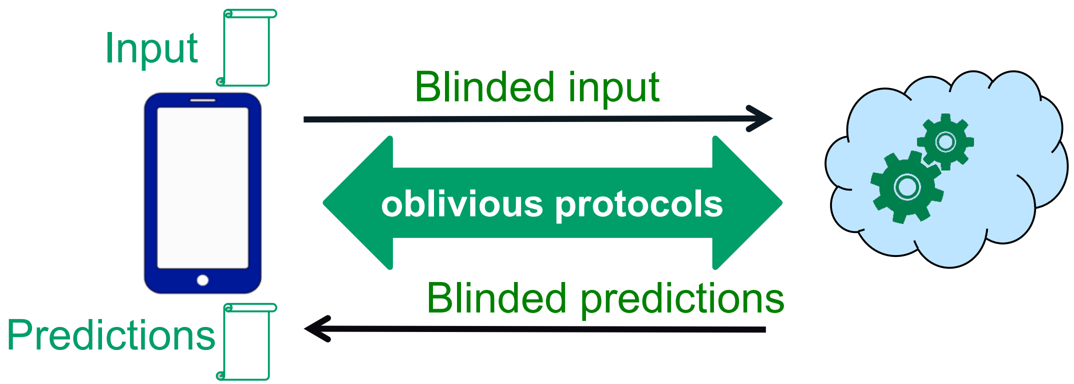
https://ssg.aalto.fi/research/projects/mlsec/

Privacy-preserving Neural Networks

How to make cloud-based prediction models preserve privacy?



violates clients' privacy



Use inexpensive cryptographic tools

MiniONN (ACM CCS 2017)

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

https://eprint.iacr.org/2017/452
https://github.com/SSGAalto/minionn

Research: Other

Building systems that are secure, usable, and deployable

Skip to Education

Skip to summary

Other themes / Emerging topics

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

- Can hardware security mechanisms help design scalable consensus schemes?

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

Securing IoT (scalability, usability) [AoF SELIoT]

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

https://ssg.aalto.fi/research/projects/seliot-project/

Stylometry and security [HICT scholarship]

- Can text analysis help detect deception?

https://ssg.aalto.fi/research/projects/deception-detection-via-text-analysis/

Automating generation of fake restaurant reviews

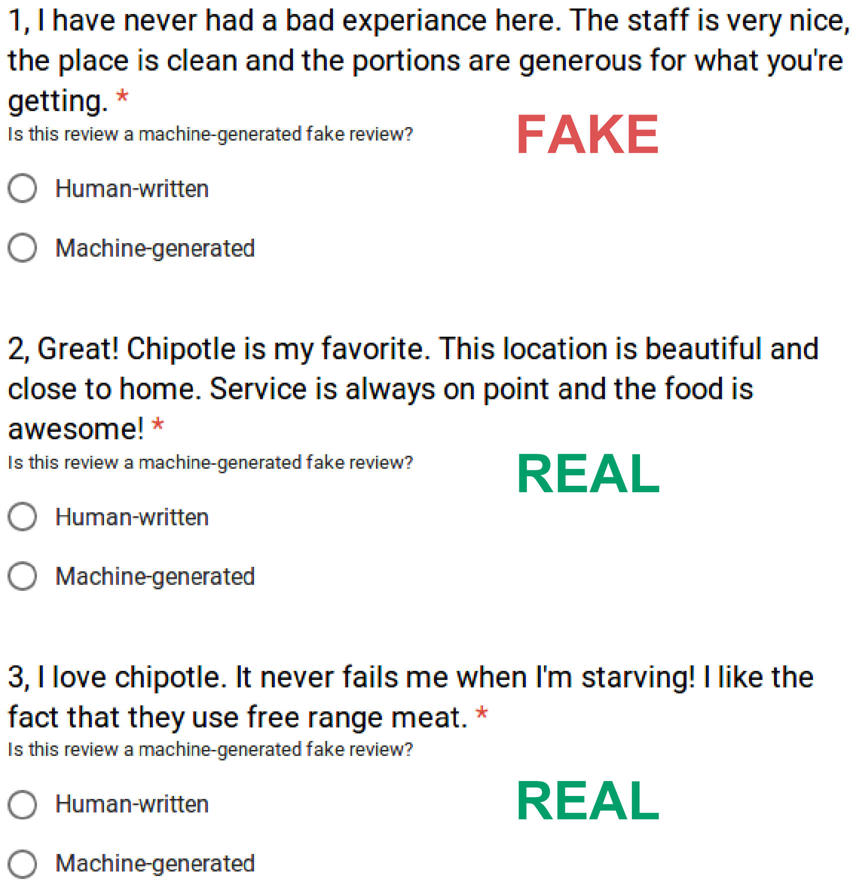
Can we machine-generate deceptive online reviews?

Generate fake reviews given a brief **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%)



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?

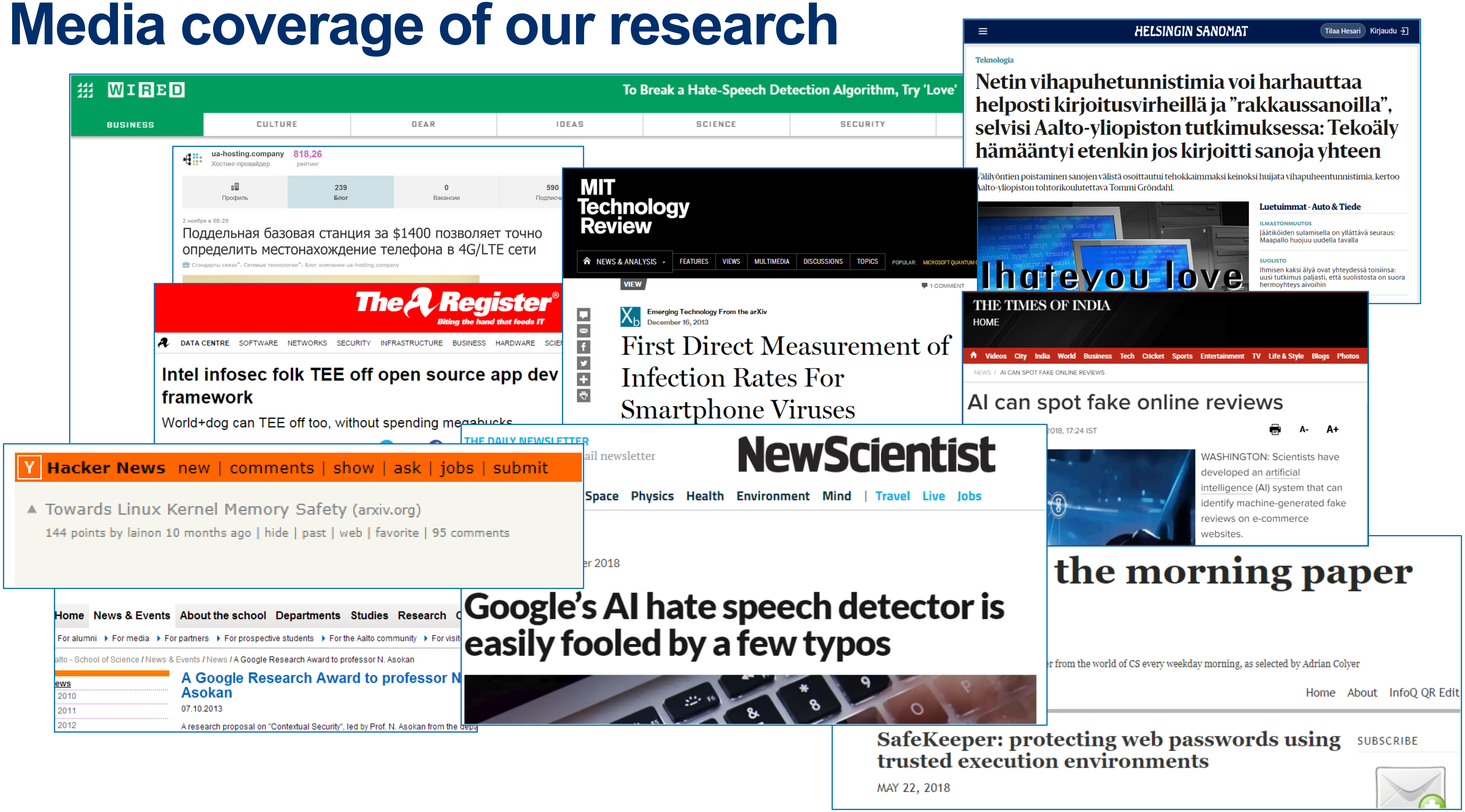
REAL

○ Human-written

○ Machine-generated

ESORICS 2018
https://arxiv.org/abs/1805.02400

Media coverage of our research



To Break a Hate-Speech Detection Algorithm, Try 'Love'

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

Intel infosec folk TEE off open source app dev framework

World+dog can TEE off too, without spending megabucks

Emerging Technology From the arXiv
December 16, 2013

First Direct Measurement of Infection Rates For Smartphone Viruses

Teknologia

Netin vihapuhetunnistimia voi harhauttaa helposti kirjoitusvirheillä ja ”rakkaussanoilla”, selvisi Aalto-yliopiston tutkimuksessa: Tekoäly hämääntyi etenkin jos kirjoitti sanoja yhteen

Välilyöntien poistaminen sanojen välistä osoittautui tehokkaimmaksi keinoksi huijata vihapuheentunnistimia, kertoo Aalto-yliopiston tohtorikoulutettava Tommi Gröndahl.

Luetuimmat - Auto & Tiede

ILMASTONMUUTOS
Jäätiköiden sulamisella on yllättävä seuraus: Maapallo huojuu uudella tavalla

SUOLISTO
Ihmisen kaksi älyä ovat yhteydessä toisiinsa: uusi tutkimus paljasti, että suolistosta on suora hermoyhteys aivoihin

AI can spot fake online reviews

2018, 17:24 IST

WASHINGTON: Scientists have developed an artificial intelligence (AI) system that can identify machine-generated fake reviews on e-commerce websites.

▲ Towards Linux Kernel Memory Safety (arxiv.org)

144 points by lainon 10 months ago | hide | past | web | favorite | 95 comments

er 2018

Google's AI hate speech detector is easily fooled by a few typos

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

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

r from the world of CS every weekday morning, as selected by Adrian Colyer

SafeKeeper: protecting web passwords using trusted execution environments

MAY 22, 2018

Research Funding (2018 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)

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

- Secure Computing, Collaborative, Autonomous and Resilient Systems

Research Institute for Collaborative
Autonomous and Resilient Systems

Blockchain Consensus and Beyond (BCon 2017 - 2020)

- Funded by Academy of Finland

Fraud detection in online commerce(2018-2019)

- Funded by Zalando Payments

Principles of industry engagement

Open IP

- **All results in the public domain (e.g., open source)**
- **Examples: Intel, Zalando**

Shared IP

- **Aalto and industry partners share IP (non-exclusive)**

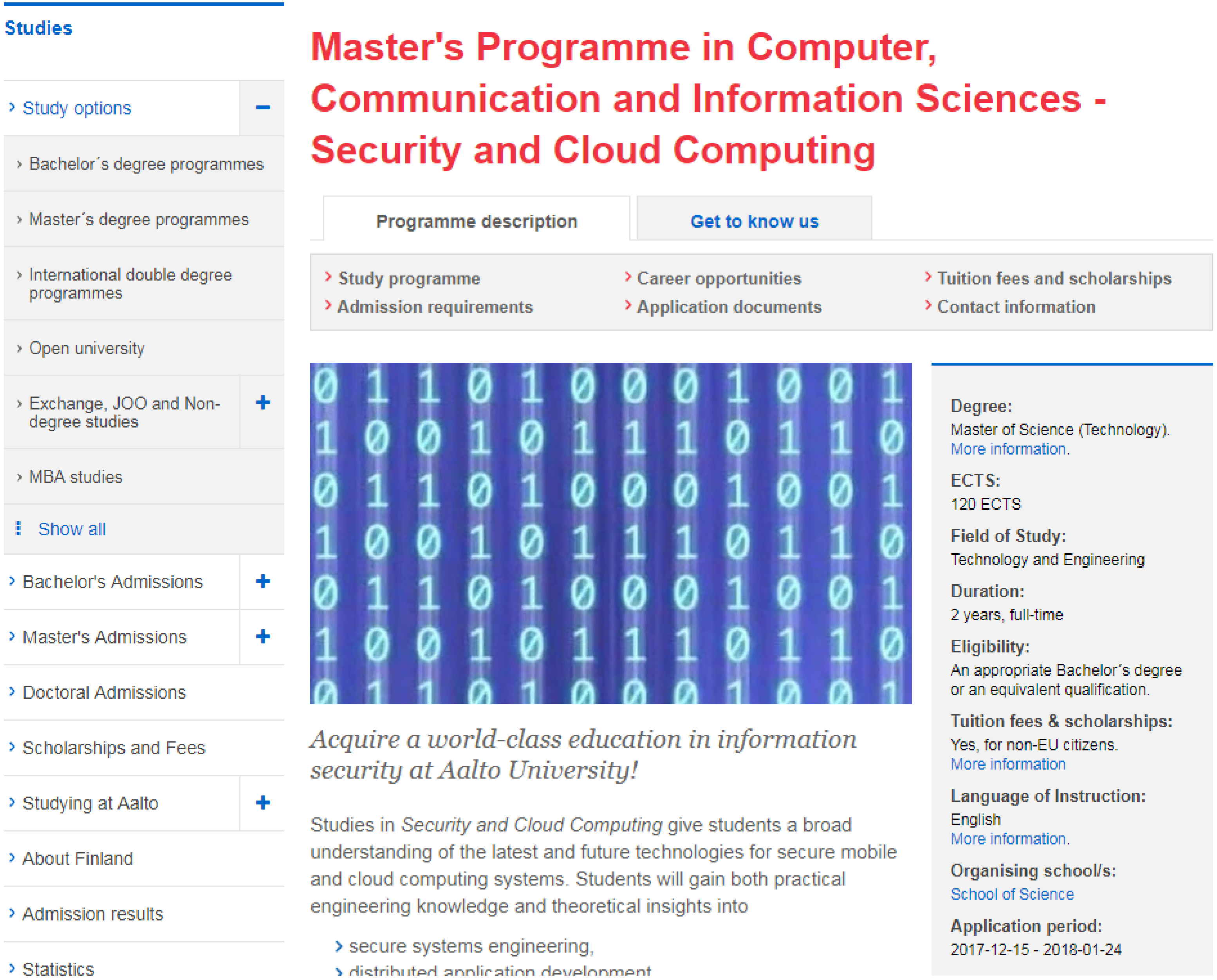
“Amplification”

- **More people working on a topic than those funded directly by industry partner**

Education

Training the next generation of information security researchers and professionals

Skip to summary



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

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

https://www.aalto.fi/ccis-security-and-cloud-computing

SECCLO

Master's Programme in Security and Cloud Computing

(Erasmus Mundus)

Applications: open in December **Scholarships available**

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

Aalto University

DTU Technical University of Denmark

EURECOM

KTH

NTNU Norwegian University of Science and Technology

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 https://haic.fi/

Mission: attract/train top students in information security

- Offers financial aid to top students in both CCIS Security and Cloud Computing & SECCLO

Call for donors and supporters

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

2018, 2019

F-Secure HUAWEI

2017

F-Secure intel nixu cybersecurity.

InfoSec Research and Education @ Aalto

20+ MSc and BSc theses yearly

2014

ACM ASIACCS (1)

PerCom (1)

Proc. IEEE (1)

ACM CCS (1)

WWW (1)

Black Hat USA (1)

Runner-up: Best CS MSc Thesis in Finland

Best InfoSec MSc thesis in Finland

2015

Black Hat Europe (1)

ACM WiSec (1)

ACM ASIACCS (1)

PerCom (1)

UbiComp (1)

ACM CCS (2)

2016

ACM CCS (1)

CeBIT (1)

NDSS (2)

Black Hat Europe (1)

IEEE ICDCS (1)

Best InfoSec MSc thesis in Finland

2017

ACM ASIACCS (1)

ACM CCS (1)

DAC (1)

IEEE IC (1)

IEEE ICDCS (2)

RAID (1)

IEEE SECON (1)

IEEE TC (1)

Best InfoSec MSc thesis in Finland

Runner-up: Best CS MSc Thesis in Finland

2018

IEEE TMC (1)

IEEE DSN (1)

WWW (1)

CT-RSA (1)

ESORICS (1)

IEEE Euro S&P (1)

DAC (1)

IEEE TC (1)

IEEE TCAD (1)

Black Hat Europe (1)

Best InfoSec MSc thesis in Finland

(awards in green)

Summary

A top systems security research group in Europe

Different possibilities for industry engagement

- **Collaborate and/or support research**
- **Support education (HAIC scholarships, internships)**

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

N. Asokan
https://asokan.org/asokan/
@nasokan