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

https://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

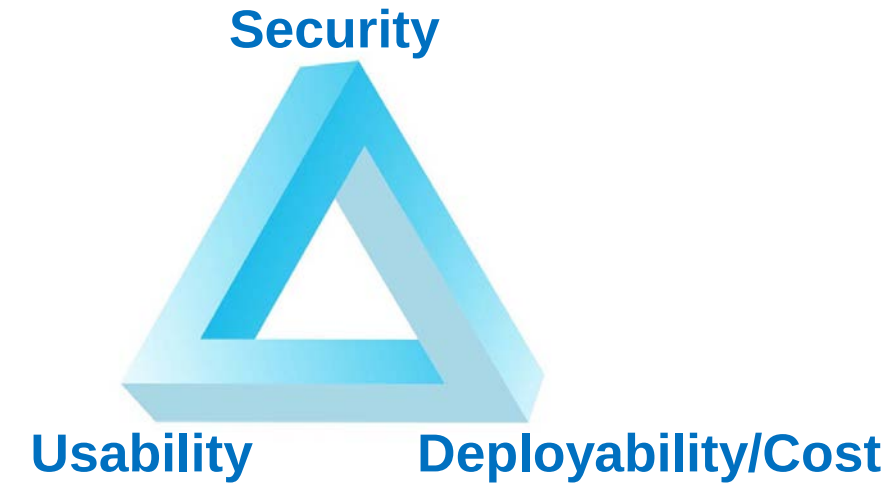
Research Fellow, Department of Computer Science

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?



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

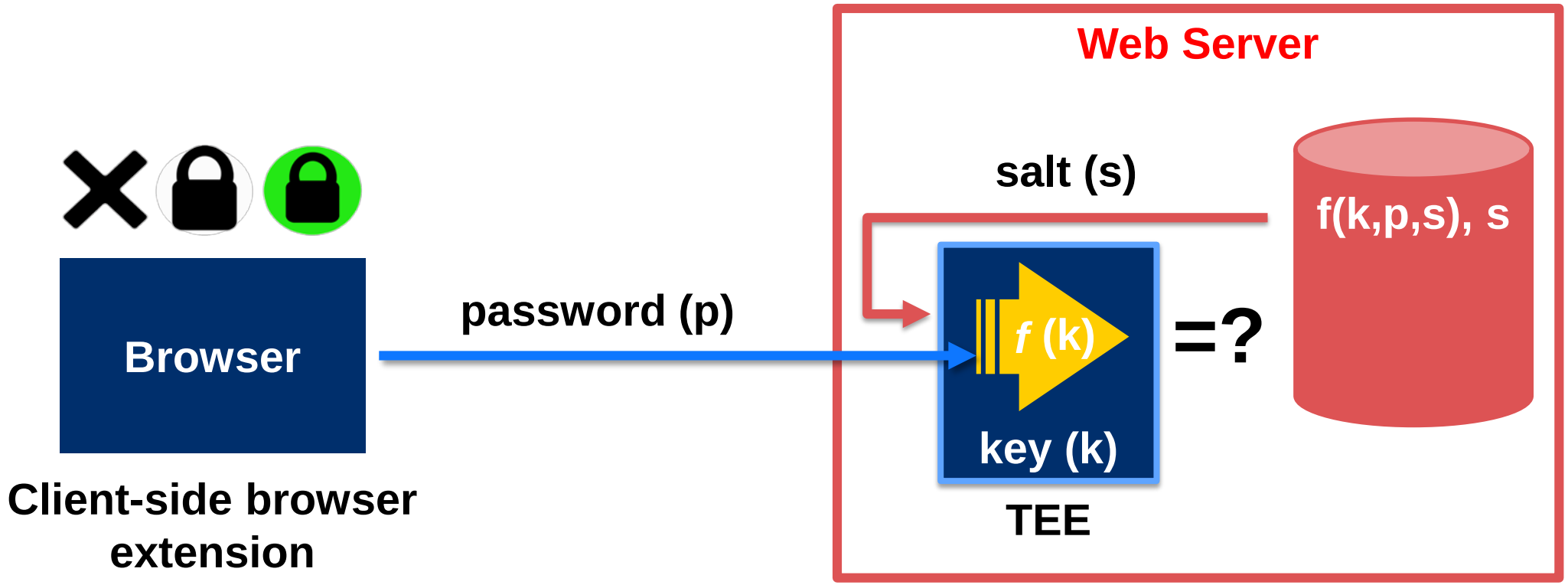
- **Examples**:
  - Protecting password-based web authentication systems
  - Breaking & repairing deniable messaging

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?



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

Breaking & repairing deniable messaging

Attestation can be used to undetectably break deniable messaging

Attestation can help restore deniability in messaging

Deniable messaging is useful…

- whistleblowers, marginalized, politicians,…

and popular

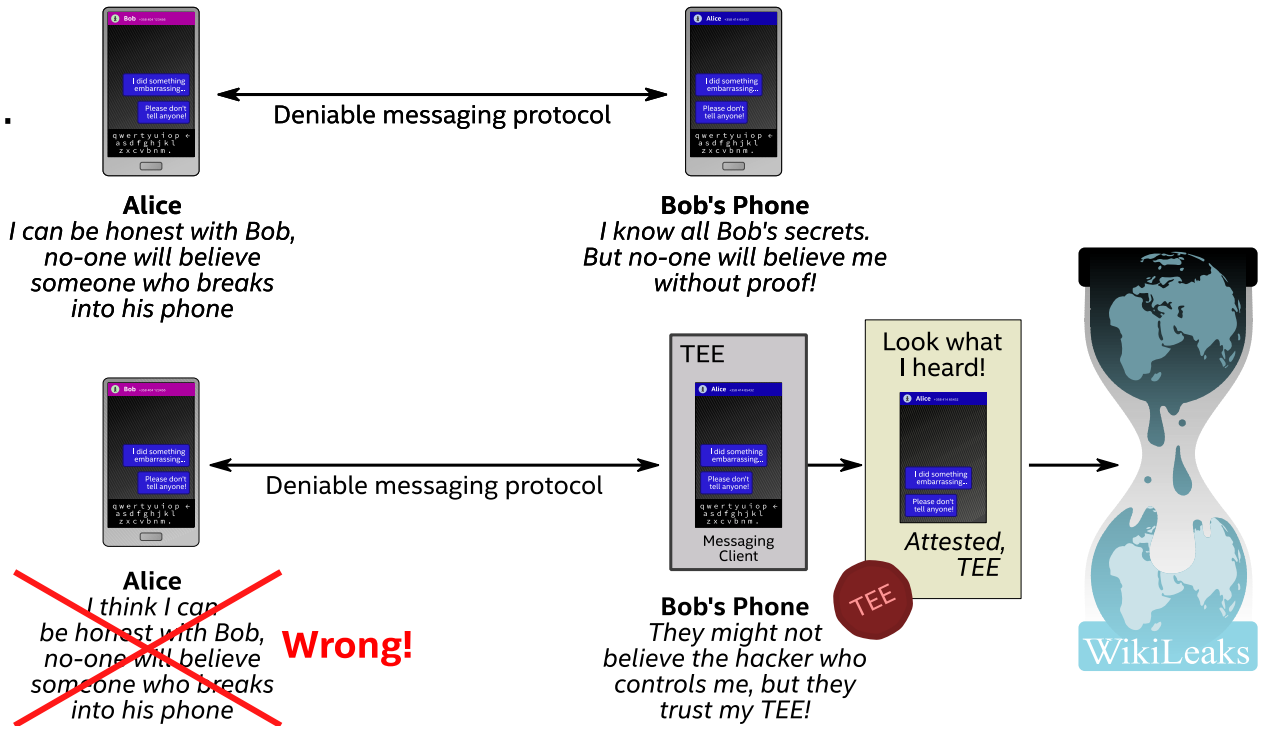
- Signal/WhatsApp, Telegram, OTR, …

Undetectably breaking deniability

- have TEE attest received messages to skeptical verifiers

S/W attacker: thwarted using attestation

- H/W attackers are hard to defend against



https://eprint.iacr.org/2018/424

Research: ML & Security

Machine learning and Security

Machine learning for security and privacy

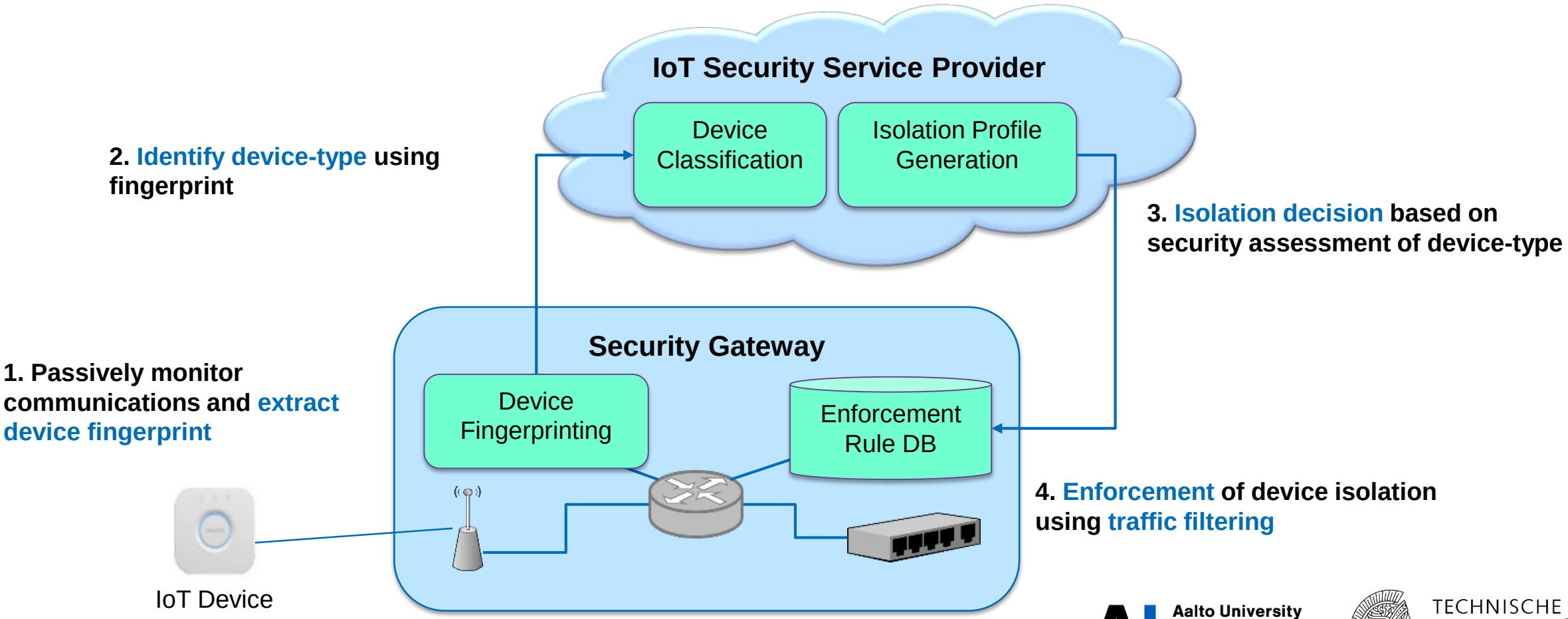
- **Examples:**
  - Fast client-side phishing detection (off-the-hook)
  - Detection of vulnerable/compromised IoT devices (IoT Sentinel and DÏoT)

Security and privacy of machine-learning based systems

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

IoT Sentinel: Automated device-type identification

How to protect smart home networks from vulnerable IoT devices?



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

DÏoT: A self-learning system for detecting compromised IoT devices

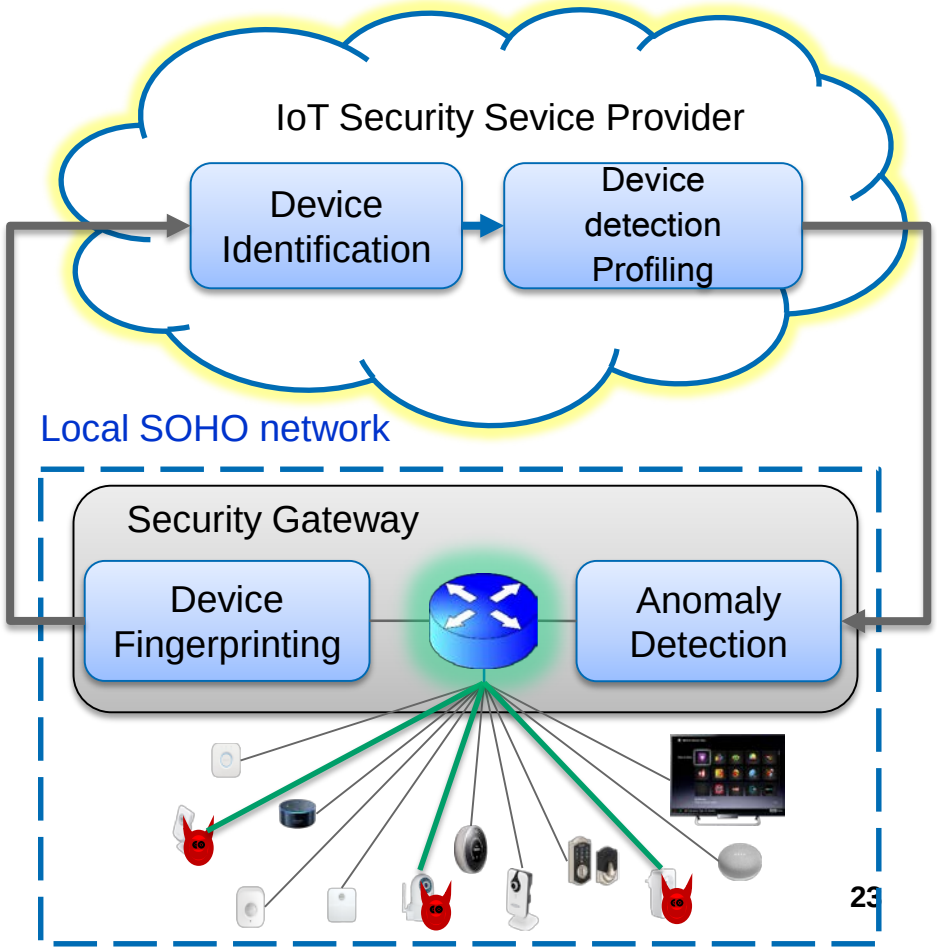
Can an IoT network autonomously detect compromised IoT devices?

DÏoT system design

- Self-learning device-type identification
- Device-type-specific anomaly detection model
- Distributed and collaborative system

Performance evaluation

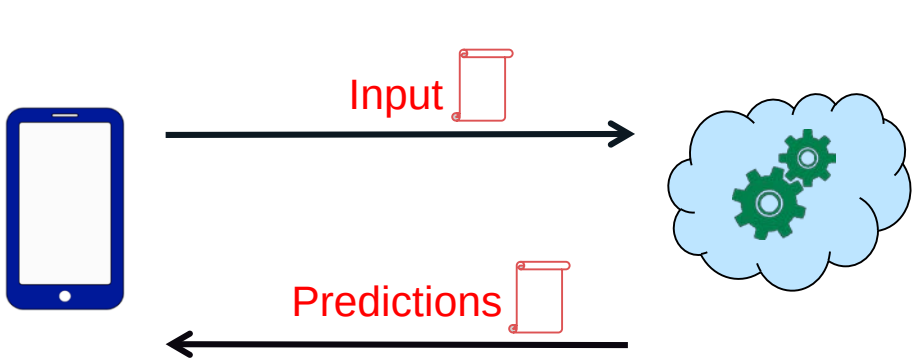
- 98% accuracy in devices-type identification
- 94% detection of Mirai (IoT botnet) attacks
- No false positives



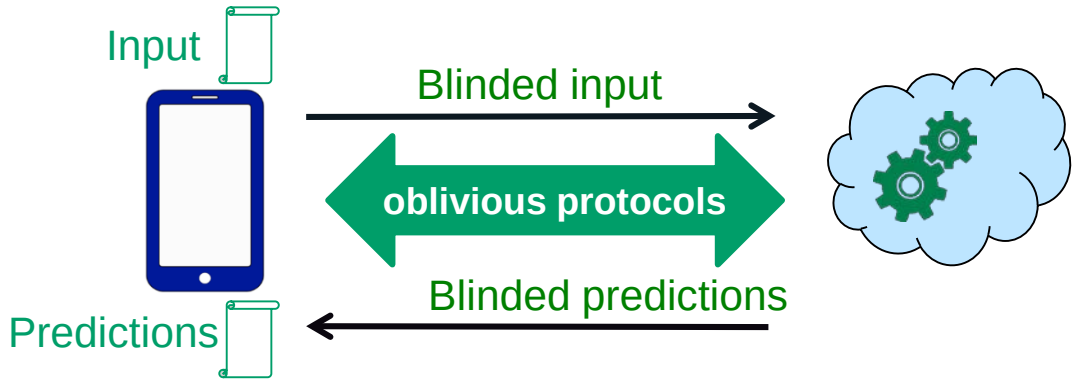
https://arxiv.org/abs/1804.07474

Privacy-preserving Neural Networks

How to make cloud-based prediction models preserve privacy?

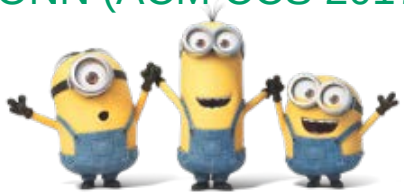


violates clients' privacy



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

Other 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?

Stay On-Topic: Generating Context-specific Fake Restaurant Reviews

How close are we to creating machine-generated deceptive online text?

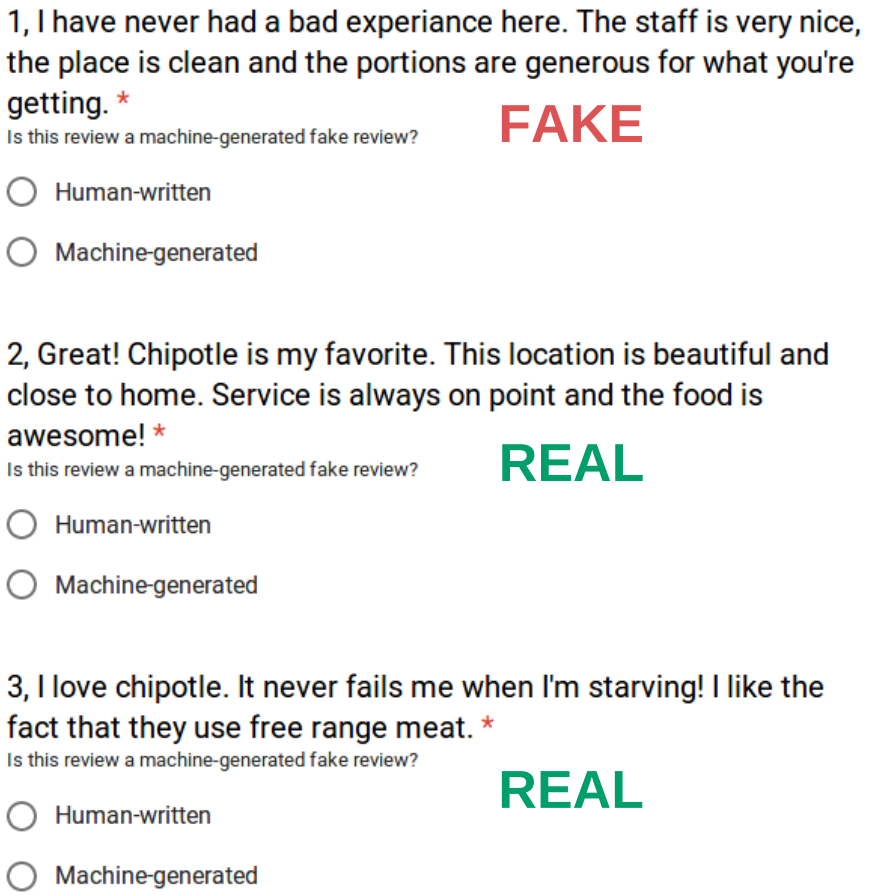
NMT-Fake* creates fake reviews from **description**:

- *5 Chipotle Mexican Grill Las Vegas NV Mexican Fast Food*

User study with **skeptical people**:

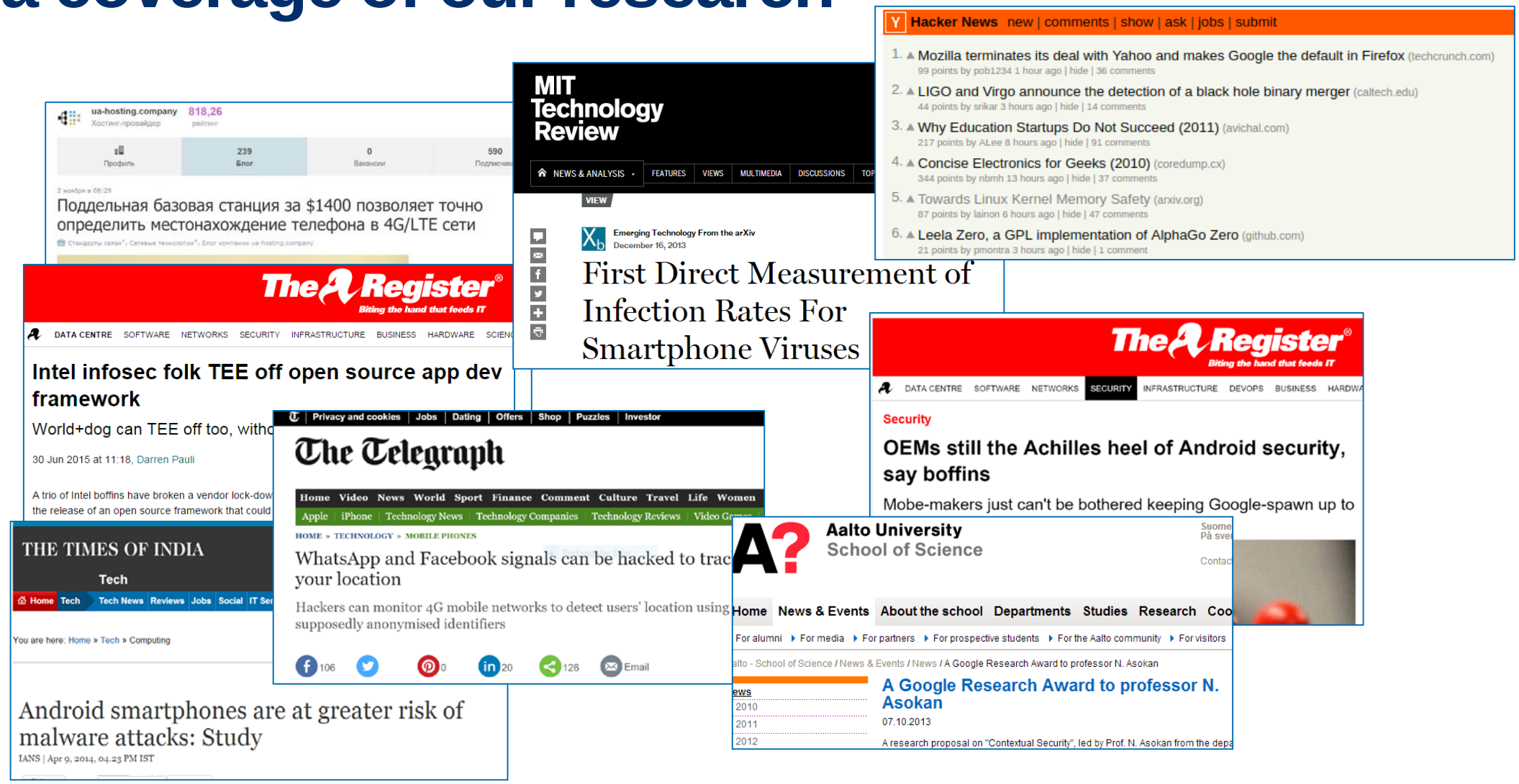
- Very poor detection, almost random (~53%)
- Detectable with machine learning (~97%)

Demo: generate your own fake restaurant reviews



https://arxiv.org/abs/1805.02400

Media coverage of our research



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/

Applications: open in December **Scholarships available**

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

Aalto University

DTU Technical University of Denmark

EURECOM

KTH

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 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

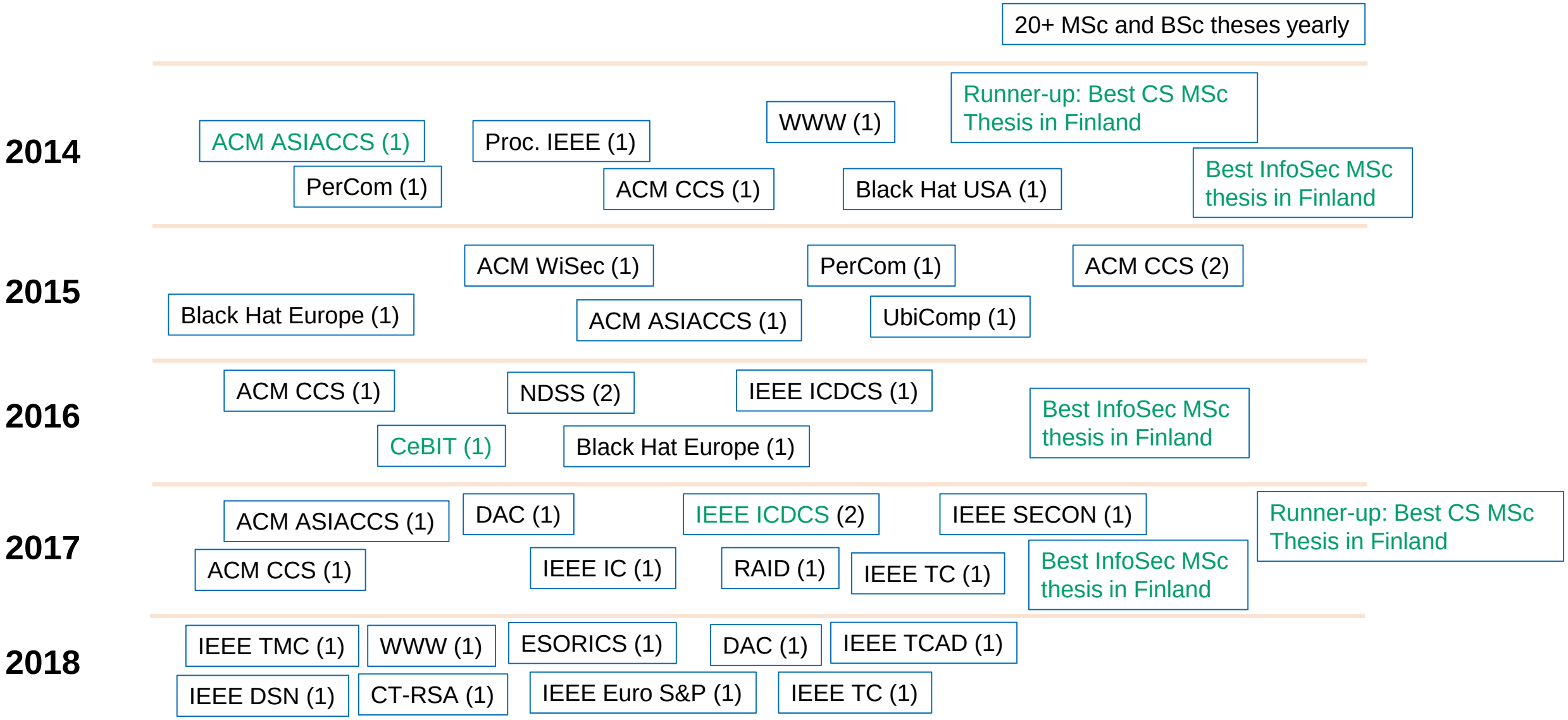
2018

F-Secure HUAWEI

2017

F-Secure intel nixu cybersecurity.

InfoSec Research and Education @ Aalto



(awards in green)

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

Information Security Research and Education at Aalto

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