

Research and Education in Information Security at Aalto University

N. Asokan



<http://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

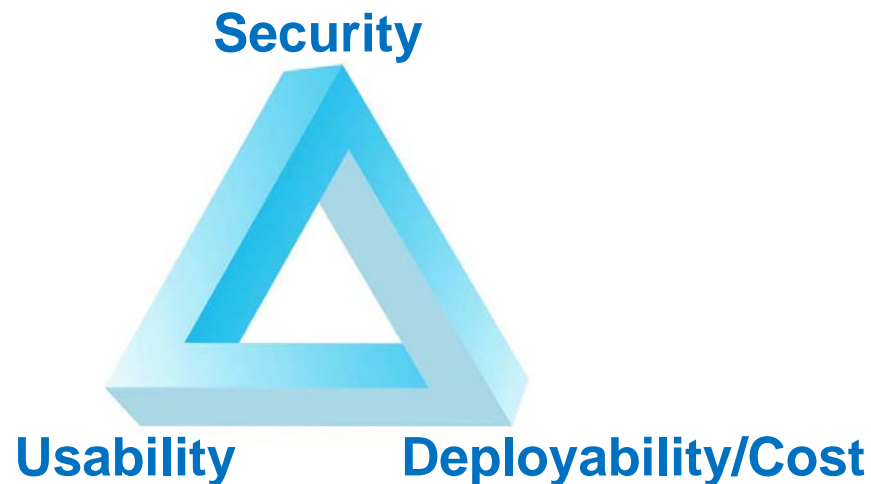
Nokia (14 y; built up Nokia security research team)

IBM Research (3 y)

<http://asokan.org/asokan/> for more background

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

Two professors: Asokan and Aura

In Asokan's projects:

- ◆ 3 postdocs
- ◆ 7 full-time PhD students
- ◆ Several MSc students

Projects funded by

Academy of Finland, Tekes

Direct industry support: E.g., Intel <http://www.icri-sc.org>,
NEC Labs



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

Current research themes: Asokan

(Mobile) Platform Security

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

Cloud Security Services

- Securely migrating local services to cloud settings

Contextual Security

- Improving security usability by leveraging contextual information

Emerging Topics

- Securing IoT and autonomous systems (scalability, usability),
Distributed consensus and blockchains (theory, applications),
5G and V2X security.

Android Malware

How pervasive is Android malware in the real world?

Project: Malware Analytics <https://ssg.aalto.fi/projects/malware/>



SE Android Analytics

How can Android OEMs securely make changes to the default AOSP SE Android policy?

Project: SE Android Analytics <https://ssg.aalto.fi/projects/seandroid-analysis/>



Linux kernel hardening

What vulnerabilities exist in the Linux kernel? How can they be mitigated?

Demo: Randomization can't stop PBF JIT spray

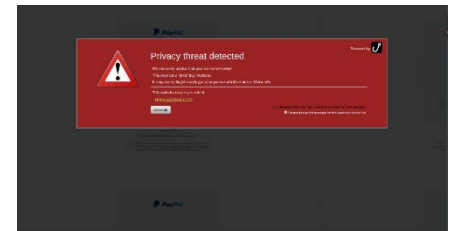
<https://www.blackhat.com/eu-16/briefings.html#randomization-cant-stop-bpf-jit-spray>

On-going work: preventing reference counter overflows and pointer bound violations

Privacy-preserving cloud-assisted services?

How can we securely transform to a cloud-assisted service model without compromising user privacy?

Project: Off-the-Hook <https://ssg.aalto.fi/projects/phishing/>



Paper: The Circle Game: Scalable Private Membership Test Using Trusted Hardware <https://arxiv.org/abs/1606.01655>

On-going activity:

- Privacy-preserving machine learning predictions

Fast consensus for block chains

Can we leverage hardware security mechanisms to design secure and scalable consensus?

Report: Scalable Byzantine Consensus via Hardware-assisted Secret Sharing <https://arxiv.org/abs/1612.04997>

InfoSec Research and Education @ Aalto

20+ MSc and BSc theses yearly

2016, 2014 Best InfoSec MSc thesis in Finland

2014 Runner-up: Best CS MSc Thesis in Finland

2014 ASIACCS (1)

2014 Proc. IEEE (1)

2014 WWW (1)

2014 PerCom (1)

2014 ACM CCS (1)

2014 Black Hat USA (1)

2015 ACM WiSec (1)

2015 PerCom (1)

2015 ACM CCS (2)

2015 Black Hat Europe (1)

2015 ASIACCS (1)

2015 UbiComp (1)

2016 ACM CCS (1)

2016 NDSS (2)

2016 ICDCS (1)

2016 Black Hat Europe (1)

2017 ASIACCS (1)

2017 DAC (1)

2017 ICDCS (2)

2017 SECON (1)

2017 IEEE TC (1)

2017 IEEE IC (1)

2017 RAID (1)

Media coverage of our research

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

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.com

MIT Technology Review

NEWS & ANALYSIS FEATURES VIEWS MULTIMEDIA DISCUSSIONS TOPICS POPULAR: MICROSOFT QUANTUM

VIEW 1 COMMENT

Xb 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 SCIENCE

Intel infosec folk TEE off open source app dev framework

World+dog can TEE off too, with...

30 Jun 2015 at 11:18, Darren Pauli

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

The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

Security

OEMs still the Achilles heel of Android security, say boffins

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

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 track your location

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

f 106 t 0 p 0 in 20 < 126 Email

A? Aalto University School of Science

Home News & Events About the school Departments Studies Research Cooperation

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

alio - 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 department of Information Systems Science

ews
2010
2011
2012

THE TIMES OF INDIA

Tech

Home Tech Tech News Reviews Jobs Social IT Services

You are here: Home » Tech » Computing

Android smartphones are at greater risk of malware attacks: Study

IANS | Apr 9, 2014, 04:23 PM IST

Recent initiatives

- Intel Collaborative Research Institute (ICRI)
 - for Secure Computing: till 2017: 610 k€ for Aalto over 3 years
 - for Collaborative, Autonomous and Resilient Systems
 - 3 years starting Fall 2017
- Securing Lifecycles of IoT devices (SELIOT)
 - Funded by NSF and Academy of Finland (WiFiUS program)
 - Aalto (Asokan), UC Irvine (Tsudik), U Florida (Traynor)
 - 2017-2019

Helsinki-Aalto Center for Information Security (HAIC)

- Joint initiative: Aalto University and University of Helsinki
- **Mission**: attract/train top students in information security
- <http://haic.aalto.fi/>
- Call for **donors** and **supporters**
 - living cost scholarships for infosec students