PROF. N. ASOKAN

May 2025

PERSONAL INFORMATION

E-mail: asokan@acm.org,asokan@ieee.org;
Web: https://asokan.org/asokan/. *X/Twitter*: @nasokan
Nationality: Citizen of Canada and Finland.

EDUCATION AND DEGREES

Doctor of Philosophy (PhD) in Computer Science *May 1998*

University of Waterloo, Waterloo, Ontario, Canada.
Dissertation title: *Fairness in Electronic Commerce.*
Supervisors: Jay Black and Michael Waidner.
Committee: Peter Landrock (external), Gord Agnew, Ken Salem, Johnny Wong.

Master of Science (MS) in Computer and Information Science *December 1989*

Syracuse University, Syracuse, New York, USA.
Subject areas: Parallel programming, the Connection Machine.

Bachelor of Technology (BTech) Honours in Computer Science & Engineering *May 1988*

Indian Institute of Technology, Kharagpur, India.
Dissertation title: *A Multi-processor Database System.*

CURRENT POSITION

University of Waterloo, Canada *From September 2019*

Full Professor (tenured) and Cheriton Chair, *David R. Cheriton School of Computer Science.*
Executive Director, Cybersecurity and Privacy Institute (CPI), *From May 2021* (on-leave during 2024)

PREVIOUS WORK EXPERIENCE

KTH, Sweden *November 2024 - December 2024*

Visiting Professor, Networked Systems Security Group.

Universiti Malaya, Malaysia *August 2024 - October 2024*

Visiting Research Associate, Faculty of Computer Science & Information Technology (FSKTM)

ETH Zürich, Switzerland *January 2024 - June 2024*

Visiting Professor, Department of Computer Science
Senior Fellow, Collegium Helveticum

Aalto University, Finland. *September 2019 - August 2024*

Adjunct Professor, *Department of Computer Science.*

Aalto University, Finland. *August 2013 - August 2019*

Full Professor (tenured), *Department of Computer Science.*
Director, Helsinki-Aalto Center for Information Security (HAIC), *June 2016 - December 2019*

University of Helsinki, Finland. *September 2012 - December 2017*

Professor (fixed term, full-time till July 2013, part-time therafter), *Department of Computer Science.*

Nokia Research Center, Helsinki, Finland. *January 1999 - September 2012*

Distinguished Researcher in security technologies, *March 2008 - September 2012*.
Distinguished Research Leader, Security and Networking Protocols team, *January 2012 - August 2012*.
Research Leader, Trustworthy Mobile Platforms, *January 2009 - December 2010*.
Research Leader, TCI team, Internet Laboratory, *May 2008 - December 2008*.
Senior Research Manager, Secure Systems group, *February 2004 - December 2006*.
Research Manager, Applied Security Technologies group, *February 2003 - February 2004*.
Principal Scientist in security technologies, *March 2000 - March 2008*.
Senior Research Engineer, *January 1999 - February 2000*.

Helsinki University of Technology, Helsinki, Finland. *March 2006 - December 2007*

Professor (fixed-term, part-time (20%) appointment), *Department of Computer Science*.

IBM Research Division, Zurich, Switzerland. *November 1995 - December 1998*

Research Staff Member, *Network security and cryptography group, Zurich Research Laboratory. January 1998 - December 1998*.

Pre-doctoral Research Scientist, *Network security and cryptography group, Zurich Research Laboratory. November 1995 - December 1997*.

University of Waterloo, Waterloo, Ontario, Canada. *January 1990 - October 1995*

Software Systems Specialist, *Mathematics Faculty Computing Facility.*

Syracuse University, Syracuse, New York, USA. *August 1988 - December 1989*

Teaching Assistant, *School of Computer and Information Science.*.

Intellisys, Syracuse, New York, USA. *May 1989 - August 1989*

Summer intern.

Hindustan Computers Ltd., Chennai, India. *May 1987 - July 1987*

Industrial trainee.

TYPES OF EXPERIENCE

Research:

University of Waterloo, Aalto University, and University of Helsinki

Systems Security: mobile platform security, machine learning and security, security of blockchains, usable security, contextual security, cloud security.

Nokia Research Center

Security Technologies: Application of data analytics to security/privacy problems, on-board credentials, security protocols for "First Connect," platform security and trusted computing, usable security, generic authentication architecture, cryptographic protocols for electronic voting and auctions, authorization protocols and infrastructures, digital rights management, security in ad hoc and disruption-prone network environments.

Networking Technologies: IPv4/IPv6 transition techniques for Mobile IP, IPv6 over GPRS, IP-based micro-mobility management.

Distributed Systems: Remote storage for mobile devices.

IBM Research Division

Electronic commerce: Generic electronic payment service, handling disputes in electronic payment systems.

Security protocols: Protocols for optimistic fair exchange, server-supported signatures, integrity protection for mobile agents, authentication of public terminals.

University of Waterloo

Security: Security issues in mobile computing.

Syracuse University

Parallel programming: Parallel implementations of algorithms and systems: the Hough transform method, Rochester connectionist simulator.

Intellisys

Image processing: A pre-processor to extract vectors out of images of text documents.

Leadership:

University of Waterloo

Leading strategic initiatives: Exective Director of Cybersecurity and Privacy Institute (CPI) (from 2021)

Leading people: Leader of Secure Systems group (part of CrySP) (from 2019)

Leading projects: PI in projects funded by NSERC (Hardware-assited security 2020-2025) and industry (including CODA/Private-AI 2021-2024, NextGenTEE 2019-2021, ICRI-CARS 2020, HARP 2019-2020)

Aalto University

Leading strategic initiatives: Founding director of Helsinki-Aalto Center for Information Security HAIC (now known as Helsinki-Aalto Institute for Cybersecurity) (2016-2019).

Leading people: Co-founder/co-director of Secure Systems group (2014-2019).

Leading projects: Lead Academic Principal Investigator, ICRI-SC (2014-2017), ICRI-CARS (2017-2020); Technical leadership of Academy of Finland (BCon, CloSe, ConSec and SELIOT) and Business Finland/Tekes (CloSer) projects.

University of Helsinki

Leading people: Founder/co-director of Secure Systems group (2012-2016).

Leading projects: Lead Academic Principal Investigator, ICRI-SC (2013-2014).

Nokia Research Center

Leading people: Line manager/Group leader, Security and Networking Protocols (2012), Trustworthy Mobile Platforms (2009-2010), TCI team (2008), Secure Systems group (2004-2006), Applied Security Technologies group (2003-2004).

Leading projects: Planning, execution, and technology transfer in several research projects.

ACM: Member of the steering group of the SIGSAC conference WiSec (2011-2015), CCS SPSM workshop (2014-2017).

Other Work Experience:

Mathematics Faculty Computing Facility, University of Waterloo

Practical network security: Development of tools and mechanisms, adaptation of Kerberos authentication system for campus use.

Other software development: Development of parts of **xhier**, a system for packaging and maintenance of software on several hundred unix systems of different flavours.

Hindustan Computers Ltd.

Software development: various projects.

EXTERNAL RESEARCH FUNDING

Summary: ∼$2.17 million CAD *external research funding* since September 2019 at the University of Waterloo:

$168 000 CAD: co-PI, Data Science Security and Privacy, ORF-RE, Province of Ontario (Total funding for the consortium of two PIs was $2 million CAD) *2023-2028*

US $310 000 (∼410 000 CAD): PI, Confidence in Distributed AI Systems, PrivateAI Institute, industry consortium led by Intel (**research gift**) 2021-2028

$70 000 CAD: PI, *Dataset watermarking*, Huawei/Canada (**research gift**) *2021*

$330 000 CAD: PI, *Hardware-assisted security*, National Science and Engineering Research Council, Canada 2020-2026

$150 000 CAD: PI, *Improving content classification performance and generalizability on small corpora*, Huawei/Finland (**research gift**) *2019-2020*

$393 000 CAD: PI, *Next generation trusted execution environments*, Huawei/Finland *2019-2021*

US $203 000 ($266 722 CAD): PI, *Intel Collaborative Research Institute for Collaborative, Autonomous and Resilient Systems* (ICRI-CARS) at UW, (**research gift**) *2020*

US $48 000 ($62 664 CAD): PI, "Hardware-assisted run-time protection", *Google ASPIRE Award 2019* (**research gift**) 2019

Summary: ∼3.5 M€ *external research funding* while at Aalto University and University of Helsinki (2013-2018):

45 000 €: PI, *Pointer Authentication*, Movial, Finland (**research gift**) *2018*

25 750 €: Co-PI (with my postdoc Dr. Samuel Marchal), "ML-based modeling of (suspicious) similarity in streaming data", *Zalando Payments*, Germany (**research gift**) *2018*

US $400 000: PI, *Intel Collaborative Research Institute for Collaborative, Autonomous and Resilient Systems* (ICRI-CARS) at Aalto, (**research gift**) *2017-2019*

419 843 €: PI, "Blockchain consensus and Beyond" (BCon), *Academy of Finland* *2017-2020*

234 894 €: Co-PI, "Securing Lifecycle of Internet of Things" (SELIOT), *Academy of Finland* 2017-2019

50 000 €: PI, "5G Security" (**research gift**), *Intel* *2016-2017*

438 500 €: Co-PI and co-ordinator, "Cloud-assisted Security Services" (CloSer), *Business Finland/Tekes* (Total funding for the consortium of 3 partners was 1.2 million €) *2016-2018*

72 120 €: PI, "Secure and Scalable Blockchain Technologies", *NEC Laboratories Europe* 2016-2017

429 921 €: PI, "Contextual Security" (ConSec), *Academy of Finland* *2014-2017*

610 000 €: Lead PI, *Intel Collaborative Research Institute for Secure Computing* (ICRI-SC) at Aalto *2014-2017*

280 011 €: PI and technical lead, "Cloud Security Services" (CloSe), *Academy of Finland* (Total funding for the consortium of 6 partners was 1.1 million €) *2014-2016*

330 000 €: PI, "Open-TEE for Android", *Huawei Corporation* *2015-2017*

US $50 000: Co-PI, Google Faculty Research Award (**unrestricted grant**) for "Contextual Security" (grant shared with Prof. Nitesh Saxena, University of Alabama at Birmingham) *2013-2014*

10 000 €: Recipient, Nokia donation for "Contextual Security" (**unrestricted grant**) *2013-2014*

200 000 €: Lead PI, *Intel Collaborative Research Institute for Secure Computing* (ICRI-SC) at University of Helsinki *2013-2014*

OTHER FUNDING

550 000 CAD: As Executive Director of CPI — Grant from Mastercard Canada to be used for research grants to CPI members, and scholarships/prizes for students. `https://cpi.uwaterloo.ca` 2023

105 000 €: As Founding Director of HAIC — Donations from industry partners (F-Secure, Huawei, Intel, Nixu) for HAIC living cost scholarships for students admitted to our MSc program. `https://haic.fi/` *2016-2018*

US $35 000: Recipient, gift from Intel for security curriculum development (**unrestricted grant**) *2013*

Project proposals inside Nokia Research Center are subject to internal evaluation/approval processes. During my career at NRC, I have **proposed and led** projects ranging from **3-5 researchers** (initial years) to **8-12 researchers** (latter years).

SUPERVISION AND MENTORING

Supervision of postdoctoral researchers:

1. *Dr. Adam Caulfield*, University of Waterloo *2024-*
2. *Dr. Uzma Maroof* (with Diogo Barradas), University of Waterloo *2023-2025*
3. *Dr. Hans Liljestrand*, University of Waterloo (to Intel Labs) *2020-2022*
4. *Dr. Mika Juuti*, University of Waterloo (to KELA, the Finnish Population Registry) *2019-2020*
5. *Dr. Jorden Whitefield*, Aalto University (to Ericsson) *2019*
6. *Dr. Saara Matala*, Aalto University (to NTNU, Norway) *2019*
7. *Dr. Lachlan Gunn*, Aalto University (to lecturer, Aalto University) *2018-2021*
8. *Dr. Mustafa Khalid Masood*, Aalto University (to Aalto U School of Engineering) *2018*
9. *Dr. Andrey Shorov*, Aalto University (to U Helsinki) *2017*
10. *Dr. Andrew Paverd*, Aalto University (to Microsoft Research) *2015-2018*
11. *Dr. Samuel Marchal*, Aalto University (to F-Secure) *2015-2019*
12. *Dr. Ravishankar Borgaonkar*, Aalto University (to Oxford) *2015*
13. *Dr. Hien Truong*, University of Helsinki (to NEC Labs Europe) *2013-2016*
14. *Dr. Sourav Bhattacharya*, Aalto University (to Bell Labs) *2014*
15. *Dr. Sini Ruohomaa*, University of Helsinki (to Ericsson) *2013-2014*

Supervision of doctoral research:

1. *Ruizhe Zhang* (with Meng Xu), University of Waterloo *In progress*
2. *Michael Wrana* (with Diogo Barradas), University of Waterloo *In progress*
3. *Vasisht Duddu*, University of Waterloo *In progress*
4. *Parjanya Vyas* (With Yousra Aafer), University of Waterloo *In progress*
5. *Hossam ElAtali* University of Waterloo, *In progress*
6. *Sebastian Szyller*, Aalto University "Ownership and Confidentiality in Machine Learning"; **Winner**: School of Science Dissertation Award, **Winner**: Finnish AI Dissertation Award *2023*
7. *Buse Atli Gul*, Aalto University "Securing Machine Learning: Streamlining Attacks and Defenses Under Realistic Adversary Models" *2022*
8. *Tommi Gröndahl*, Aalto University "Natural Language Processing in Adversarial Settings and Beyond: Benefits and Risks of Text Classification, Transformation, and Representation" (now postdoctoral researcher, University of Helsinki) *2022*
9. *Arseny Kurnikov*, Aalto University "Trusted Execution Environments in Cloud Computing" (now Engineer, Ericsson) *2022*
10. *Thomas Nyman*, Aalto University, "Toward hardware-assisted run-time protection" (now Engineer, Ericsson) *2020*
11. *Hans Liljestrand*, Aalto University, "Hardware-assisted memory safety" (now Intel Labs) *2020*
12. *Mika Juuti*, Aalto University, "Access Control and Machine Learning: Evasion and Defenses" (now Senior Data Scientist, KELA, the Finnish Population Registry) *2019*

13. *Jian Liu* "Privacy-Preserving Cloud-Assisted Services", Aalto University, *Pass with distinction.* (now Assistant Professor, Zhejiang University) *2018*
14. *Elena Reshetova*, , Aalto University, "Mobile and Embedded Platform Security" (now Senior Engineer, Intel) *2018*
15. *Sandeep Tamrakar*, Aalto University, "Applications of Trusted Execution Environments (TEEs)", (now Senior Engineer, Huawei Technologies) *2017*

Supervision of doctoral research, as advisor (formally "advisor" ('ohjaaja'), effectively de-facto supervisor including guidance of day-to-day research, joint publications):

16. *Marcin Nagy*, Aalto University, "Secure and Usable Services in Opportunistic Networks" (now Product Director, IoT-AVSystem) *2019*
17. *Jan-Erik Ekberg*, Aalto University, "Securing Software Architectures for Trusted Processor Environments", Aalto University. (now CTO for Mobile Security, Huawei Technologies) *2013*
18. *Kari Kostiainen*, Aalto University, "On-board Credentials: An Open Credential Platform for Mobile Devices", Aalto University. *Pass with distinction ('kiittäen hyväksytty').* (now Senior researcher, ETH Zürich) *2012*

Supervisor: Masters theses:

(as Professor at University of Waterloo)

1. *Prach Chantasantitam*, in progress *2026*
2. *Anudeep Das*, in progress *2026*
3. *Mehdi Aghakishiyev* (with Meng Xu), in progress *2025*
4. *Ruizhe Wang* (with Meng Xu), "Efficient Memory Allocator for Restricting Use-After-Free Exploitations" *2024*
5. *Owura Asare* (with Mei Nagappan), "Security Evaluations of GitHub's Copilot" *2023*
6. *Asim Waheed*, "On Using Embeddings for Ownership Verification of Graph Neural Networks" *2023*
7. *Xiaohe Duan*, "Compiler-Based Approach to Enhance BliMe Hardware Usability" *2023*
8. *Shelly Wang*, "Security and Ownership Verification in Deep Reinforcement Learning" *2022*
9. *Setareh Ghorshi*, "SafeDS: Safe Data Structures for C++" *2022*
10. *Vasisht Duddu*, "Towards Effective Measurement of Membership Privacy Risk for Machine Learning Models" *2022*
11. *Karthik Ramesh*, "Multimodal spoofingng and adversarial examples countermeasure for speaker verification" *2022*

(as Professor at Aalto University)

12. *Yujia Guo*, "Symbolic Computation in Deep Neural Networks" *2022*
13. *Eleonora Micozzi*, "Guarantees of Differential Privacy in Overparameterised Models" *2021*
14. *Minh Duc Hoang*, "Dataset Watermarking" *2021*
15. *Max Crone*, "Towards Attack-tolerant Trusted Execution Environments" *2021*
16. *Yuxi Xia*, "Watermarking Federated Deep Neural Network Models" *2020*
17. *Sebastian Szyller*, "Adversary Detection in Online Machine Learning Systems" *2020*

18. *Martin Kulhavy*, "Efficient Collection and Processing of Cyber Threat Intelligence from Partner Feeds" *2019*
19. *Broderick Acquilino*, "Relevance of Security Features Introduced in Modern Windows OS" *2019*
20. *Markus Lehtonen*, "Cyber Threat Intelligence Management: a Triage and Analysis " *2019*
21. *Andrei Kazlouski*, "Text style imitation to prevent author identification and profiling" *2019*
22. *Mari Nikkarinen*, "Security in Authentication Systems and How Usability and Human Factors Contribute to Security in OneID" *2019*
23. *Raine Nieminen*, "Privacy-Preserving Indoor Localization with Paillier Encryption and Garbled Circuits" *2018*
24. *Max Reuter*, "Privacy Preserving Deep Neural Network Prediction using Trusted Hardware" *2018*
25. *Ricardo Vieitez Parra*, "The Impact of Attestation on Deniability" *2018*
26. *Koen Tange*, "High Speed Consensus with Trusted Execution Environments" *2018*
27. *Sten Hägglund*, "Impact of European Union General Data Protection Regulation to Software-as-a- service Providers" *2018*
28. *Johannes Vainio*, "Physically Unclonable Functions as Trust Anchors for Connected Embedded Device Security" *2018*
29. *Artur Valiev* "Automatic Ownership Change Detection for IoT devices" *2018*
30. *Alexey Dmitrenko*, "DNN Model Extraction Attacks using Prediction Interfaces" *2018*
31. *Dmitry Kiritchenko*, "Detection of Application used on a Mobile Device Based on Network Traffic" *2018*
32. *Manish Thapa*, "Mitigating Threats in IoT Network using Device Isolation" *2018*
33. *Anwar Hassan*, "Detecting Botnets in OpenStack Cloud Environment" *2017*
34. *Radek Tomšů*, "Automated Deauthentication using Web Transaction Analysis, *2017*
35. *Buse Gül Atli*, "Anomaly-Based Intrusion Detection by Modeling Probability Distributions of Flow Characteristics", *2017*
36. *Rakesh Gopinath*, "Improving the Security and Efficiency of Blockchain-based Cryptocurrencies" *2017*
37. *Md Sakib Nizam Khan*, "Enhancing Privacy in IoT devices through Automated Handling of Ownership Change" *2017*
38. *Klaudia Krawiecka*, "Improving Web Security using Trusted Hardware" **Winner**, Best information security thesis in Finland (Tietoturva ry), **Honourable Mention**, Best computer science thesis in Finland (Finnish Society for Computer Science). *2017*
39. *Gayathri Srinivaasan*, "Malicious Entity Categorization using Graph Modeling" *2016*
40. *Giovanni Armano*, "Real-Time client-side phishing prevention" *2016*
41. *Dawin Schmidt*, "A Security and Privacy Audit of KakaoTalk's End-to-end Encryption" *2016*
42. *Luigi di Girolamo*, "Design and development of an Android access management application" *2016*
43. *Rui Yang*, "Java APIs for trusted execution environments" *2016*
44. *César Pereída*, "Cache-timing techniques: exploiting the DSA algorithm" **Winner**, Best information security thesis in Finland (Tietoturva ry) *2016*
45. *Pävivi Tynninen*, "Towards automated isolation of security sensitive execution" *2016*
46. *Lari Lehtomäki*, "Realizing eID scheme on TPM 2.0 hardware" *2016*
47. *Swapnil Udar*, "Contextual Authentication and Autho- rization using Wearable Devices" *2016*

48. *Setareh Roshan Kokabha*, "An Online Anomaly-Detection Neural Networks-based Clustering for Adaptive Intrusion Detection Systems" *2015*
49. *Nguyen Hoang Long*, "Securely accessing encrypted cloud storage from multiple devices" *2015*
50. *Robin Babujee Jerome*, "Pre-processing Techniques for Anomaly Detection in Telecommunication Networks". *2015*

(as Professor at University of Helsinki)

51. *Aaro Lehikoinen*, "HardScope: Defence Against Data-oriented Programming Attacks" *2017*
52. *Aku Silvennoinen*, "Accountable De-anonymization in V2X Communication" *2017*
53. *Hans Liljestrand*, "Linux Kernel Memory Safety" **Winner**, Best information security thesis in Finland (Tietoturva ry) *2017*
54. *Jian Liu*, "How to Steer Users Away from Unsafe Content". *2014*
55. *Xiang Gao*, "Strengthening Zero-Interaction Authentication Using Contextual Co-presence Detection". *2014*
56. *Thomas Nyman*, "Dynamic Isolated Domains" *2014*

(as Professor at Helsinki University of Technology)

57. *Pekka Sillanpää*, "Distributed Digital Identity System – Peer-to-Peer Perspective" *2007*
58. *Aishvarya Sharma*, "On-board Credentials: Hardware assisted secure storage of credentials" *2007*
59. *Cherdpan Sripan*, "User-to-Service authentication Using Mobile phones" *2006*
60. *Antti Halla*, "Applying a Systems Approach to Security in a Voice Over IP System" *2006*
61. *Otto Kolsi*, "Secure MIDP Applications". *2006*

Supervision of MSc theses, as advisor (formally 'advisor' ('ohjaaja'), effectively de-facto supervisor including guidance of day-to-day research, joint publications):

1. *Olli Jarva*, "Intelligent two-factor authentication – Deciding authentication requirements using historical context data"", Aalto University.
   Winner, Best information security thesis in Finland (Tietoturva ry), **Honourable Mention**, Best computer science thesis in Finland (Finnish Society for Computer Science). *2014*
2. *Kari Kostiainen*, "Intuitive Security Initiation Using Location-Limited Channels", Helsinki University of Technology. *2004*
3. *Jarkko Tolvanen*, "Device Security", University of Helsinki. *2001*

Supervision of graduate research interns: These interns typically spent 4-6 months in my group at Nokia Research Center under my guidance (sometimes also under the guidance of a senior researcher in my group). Many of the students went on to do follow-up work in the same or related areas. In several cases (marked with an '*'), the intern's work done under my supervision was included in the eventual thesis/dissertation.

1. * *Marcin Nagy* (Aalto, doctoral)
2. * *Aditi Gupta* (Purdue, doctoral)
3. *Alexandra Afanasyeva* (SUAI St. Petersburg, doctoral)
4. * *Pern Hui Chia* (NTNU, doctoral; Helsinki University of Technology, master's)
5. * *Sandeep Tamrakar* (Aalto; doctoral)

6. * *John Solis* (UC Irvine; doctoral)
7. * *Paul Dunphy* (Newcastle; doctoral)
8. * *Long Nguyen Huang* (Helsinki University of Technology; master's)
9. * *Ersin Uzun* (UC Irvine; doctoral)
10. *Nitesh Saxena* (UC Irvine; doctoral)

TEACHING

Teaching – coursework:

University of Waterloo

CS 858 Selected topics in system security *Winter 2021, 2022, 2023*
CS 458/658 Computer Security and Privacy *Spring 2020, 2021*

Aalto University

CS-E4310 Mobile Systems Security. (annually) *Spring 2015-2020*

GIAN program, Ministry of Human Resource Development, India

Mobile Systems Security, MNIT Jaipur. *Nov 2016*

University of Helsinki

Mobile Platform Security. *Spring 2014*
Research seminar on Mobile Security. *Fall 2013*
Undergraduate seminar: Information and System Security. *Spring 2013*
Mini course: Selected topics in mobile security *Fall 2012*
Undergraduate seminar: Security in distributed systems. *Fall 2000*

Universitá degli Studi di Padova

Lectures for European Commission Erasmus "Lifelong Learning Programme" *July 2012*

Helsinki University of Technology

T-110.6120 Undergraduate seminar: Special course in data communication software (responsible for security-related topics). *Fall 2006, 2007*
T-110.7190 Research Seminar on Data communications Software: Energy Awareness (responsible for security-related topics). *Fall 2007*
T-110.7200 Graduate Research Seminar: Recent Advances in Trustworthy Computing. *Spring 2007*
T-110.7290 Graduate Research Seminar: Authentication and Key Establishment (with Kaisa Nyberg, T-79.7001). *Fall 2006*

Syracuse University

Introduction to pascal programming (adult education section). *Fall 1989*
Introduction to pascal programming. *Spring 1989*
Teaching Assistant, Introduction to pascal programming. *Fall 1988*

Indian Institute of Technology, Kharagpur

Laboratory instructor, Programming and data structures course. *Spring 1988*

Teaching – course development: Mobile Systems Security. *Spring 2014*

Teaching – tutorials:

1. *Remote Attestation – Building trust in things you can't see*, Tutorial at **ACM Asia Conference on Computer and Communications Security** (ASIACCS 2017), Abu Dhabi, UAE, April 2017
2. *Challenges in Realizing Secure Cloud Storage Services*, Lecture at the **Summer School on Secure and Trustworthy Computing**, Bucharest, Romania, `http://summerschool.trust.cased.de/` *Sep 2015*

3. *Mobile Security*, 3 lectures at the **International Summer School on Information Security**, Bilbao, Spain, http://grammars.grlmc.com/InfoSec2015/ *July 2015*
4. *Mobile Security*, 3 lectures at the **Third TCE Summer School on Computer Security**, Technion, Israel, http://events-tce.technion.ac.il/summer-school-2014/ (videos: https://youtu.be/PFjh-IeUJMI, and https://youtu.be/MHZZ84gWH_c) *September 2014*
5. *Mobile Security*, 3 lectures at the **International Summer School on Smart & Mobile Device Security and Privacy**, Padova, Italy. http://spritz.math.unipd.it/events/2014/SMDSP/index.html *September 2014*
6. *Mobile Platform Security Architectures*, Half day tutorial, **International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2012)**, Indian Institute of Technology, Chennai, India. *October 2012*
7. *Security for end users: from personal devices to Internet of Things*, (Planned) Half day tutorial, **International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2012)**, Indian Institute of Technology, Chennai, India. *October 2012*
8. *Intuitive security policy configuration in mobile devices using context profiling* (Invited Guest Speaker Talk), **6th Bertinoro PhD School on Security of Wireless Networking**, Bertinoro, Italy. October 2012
9. *Initializing Security Associations for Personal Devices*, **ZISC workshop on Wireless Security**, ETH Zürich, Switzerland. *September 2007*

AWARDS AND HONOURS

Distinguished paper award, IEEE Security and Privacy Symposium, https://sp2024.ieee-security.org/awards.html *2024*

Fellow of the Royal Society of Canada
https://rsc-src.ca/en/news/press-release-rsc-presents-class-2023 *2023*

Outstanding Performance Award, University of Waterloo https://uwaterloo.ca/daily-bulletin/2023-06-08#2022-outstanding-performance-award-recipients-named *2023*

Best paper award, IEEE Transactions on Computers
https://www.computer.org/publications/best-paper-award-winners *2019*

ACM Fellow https://awards.acm.org/fellows/award-winners *2018*

ACM SIGSAC Outstanding Innovation Award, *2018*
https://www.sigsac.org/award/sigsac-awards.html

Finalist, NYU CyberSecurity Awareness week (CSAW) Applied Research Competition, *2017*
https://csaw.engineering.nyu.edu/research

Best poster/demo award, IEEE ICDCS 2017 conference, https://research.aalto.fi/en/prizes/ieee-icdcs-201 *2017*

Honorable Mention, ACM ASIACCS 2017 conference
http://asiaccs2017.com/program/distinguished-papers/ *2017*

IEEE Fellow (http://www.comsoc.org/about/memberprograms/fellows/2017) *2017*

First prize (20 000 €) for OmniShare in the EU MAPPING "Privacy via IT Security" App Competition, awarded at CeBIT. http://www.mappingtheinternet.eu/node/115 *2016*

Best small course (responsible professor) and second best small course (lecturer and responsible professor) as rated by students, Computer Science department, Aalto University. https://wiki.aalto.fi/display/CSnews/CS+News#CSNews-ThebestcoursesoftheDegreeProgrammeinCSE *2015*

ACM Distinguished Scientist. http://awards.acm.org/award_winners/asokan_4672457.cfm *2015*

Best paper award, ACM ASIACCS 2014 conference. http://asiaccs2014.nict.go.jp/ *2014*

Google Faculty Research Award. *2013*
https://research.google/outreach/past-programs/faculty-research-awards/?category=2013

Best demo award, IEEE PerCom 2011 conference. *2011*

Nokia Excellence Award – Research Category, Leader of a semi-finalist team (top 12/57), Nokia *2011*

NRC Breakthrough[1] (**Device Certification Server** technology transfer), Nokia. *Dec. 2010*

NRC Breakthrough (**On-board Credentials for Symbian** technology transfer), Nokia. *Jun. 2010*

Best paper award, INTRUST 2009 conference. *2009*

Induction into Nokia Research Center Club-10 (Holders of 10 Nokia patents), Nokia. *2007*

Nokia Quality Award – Research Category, Member of a finalist team (top 3), Nokia. *2007*

Inventor of the Year, Nokia. *2005*

Nokia Quality Award – Research Category, Member of the winning team, Nokia. *2005*

Research Division Award, IBM Research Division. *1998*

First Patent Application Award, IBM Research Division. *1998*

Graduate Scholarship, Syracuse University. *1988-89*

Summer Fellowship, Syracuse University. *Summer 1989*

SERVICE TO SCIENTIFIC/TECHNICAL COMMUNITY

Editorial boards and steering committees:

Guest editor, Special issue on hardware-assisted security, IEEE *Security and Privacy*. *2020*
Associate Editor (2016) and Associate Editor-in-Chief (2017), IEEE *Security and Privacy*. *2016-2017*
Associate Editor, ACM Transactions on Information and System Security (TISSEC) *2013-2016*
Proceedings on Privacy Enhancing Technologies (PoPETs). *2014-2015, 2016-2017*
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM). *2013-2017*

[1] An "NRC breakthrough" is a technology transfer activity whose net present value is evaluated to be over 10 million € by a Nokia operating unit and the NRC Business Validation team.

ACM Conference on Security and Privacy in Wireless and Mobile Networks. *2011-2015*
Computer Communications Journal. *2009-2010*
IEEE *Network*. *2007-2011*

Program chairs:

ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM). *2013*
International Conference on Trust and Trustworthy Computing – Technical Track (TRUST). *2013*
ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec). *2011*
ACM Workshop on Scalable Trusted Computing (ACM STC). *2009, 2010*

Program committees:

The Web Conference (formerly "WWW Conference"). *2019*
ACM Symposium on Information, Computer and Communications Security (ACM ASIACCS). *2008-2010, 2015, 2017*
IEEE International Conference on Pervasive Computing and Communications (PerCom) *2015-2016*
IEEE International Conference on Distributed Computing Systems (ICDCS) *2014*
Smart Card Research and Advanced Application Conference (CARDIS) conference *2012,2013*
International Conference on Trusted Systems (INTRUST). *2009-2010*
International Conference on Trust and Trustworthy Computing (TRUST). *2008, 2010*
ACM Workshop on Scalable Trusted Computing (ACM STC). *2008-2009*
ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec). *2008, 2010, 2013*
Financial Cryptography and Data Security. *2008-2009, 2016*
ACM Digital Rights Management Workshop (ACM DRM). *2007*
Nordic Workshop on Secure IT Systems (Nordsec). *2007, 2010*
SKLOIS Conference on Information Security and Cryptology (Inscrypt). *2006*
International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm). *2005-2008*
Secure Mobile Ad-hoc Networks and Sensors workshop (MADNES). *2005*
International Conference Security in Pervasive Computing (SPC). *2003-2006*
European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS). *2004-2007*
International Conference on Applied Cryptography and Network Security (ACNS). *2004, 2011*
Information Security Conference (ISC). *2003, 2006*
IEEE Workshop on Wireless Local Networks (WLN). *2002-2003*
European Symposium on Research in Computer Security (ESORICS). *2000*
ACM Conference on Computer and Communications Security (ACM CCS). *1999*

Direct contribution to standardization:

Bluetooth Special Interest Group: Bluetooth Secure Simple Pairing specification. (included in Bluetooth 2.1) *2007*

USB Implementors Forum: Association Models Supplement to the Certified Wireless Universal Serial Bus Specification. *2006*

Indirect contribution to standardization:

3GPP SA3, Security Working Group: Generic Authentication Architecture. *2002-2006*

CE4A: Terminal Mode (later "MiirorLink") Technical Architecture v1.0. *2004-2006*

Dissertation committees/Dissertation examinations:

Habilitation level: Dr. Melek Önen (Eurecom, 2017)

Doctoral level: Andre Kassis (UWaterloo, on-going); Thien Nguyen (TU Darmstadt, 2024), Nils Lukas (UWateroo, 2024), Bailey Kacsmar (UWaterloo, 2023), Patrick Jauering (TU Darmstadt, 2023), Emmanuel Stapf (TU Darmstadt, 2022), Simon Birnbach (Oxford, 2022), Jiayi Chen (UWaterloo, 2022), Masoumeh Shafieinejad (UWaterloo, 2021), Ágnes Kiss (TU Darmstadt, 2020), Markus Miettinen (TU Darmstadt, 2018), Carlton Sheppard (Royal Holloway, 2018), Pawani Porambage (University of Oulu, 2018), Michael Hölzl (Johannes Kepler University, 2018), Vincent Taylor (Oxford University, 2017), Nicolae Paladi (Lund University of Technology, 2017), Stephan Heuser (TU Darmstadt, 2016), Babins Shrestha (University of Alabama at Birmingham, 2016) Claudio Marforio (ETH Zürich, 2015), Guillermo Suárez.Tabgil (Universidad Carlos III de Madrid, 2014), Nils Ole Tippenhauer (ETH Zürich, 2012), Ersin Uzun and John Solis (University of California at Irvine, 2010), Levente Buttyán, (École Polytechnique Fédérale de Lausanne, 2002), Tuomas Aura (Helsinki University of Technology, 2000).

Master's level: Stephen Asherson (University of Cape Town, 2008).

Invited service in expert groups:

Member, ACM SIGSAC Awards committee. *2023*

Member, Heidelberg Laureate Forum selection committee. *2019*

Member, IEEE Computer Society, Fellows evaluation committee.
`https://www.computer.org/web/volunteers/fellows` *2017,2020,2022*

Member, European Research Council, Starting Grant evaluation panel.
`https://erc.europa.eu/document-category/evaluation-panels` *2016-2022*

Domain expert, security/privacy group of the ACM Computing Classification System (CCS) Update Project (`http://www.acm.org/about/class/2012?pageIndex=2`). *2011*

Membership in the industrial advisory board of the European Commission research project S3MS. *2008*

Internal service:

Member, Promotions and Tenure committee, University of Waterloo School of Computer Science *2022*

Member, Performance Review committee, University of Waterloo School of Computer Science *2021-2022*

Member, Graduate Recruitment committee (GREC), University of Waterloo School of Computer Science *2020-2021*

Member, Awards committee, University of Waterloo School of Computer Science *2019-2021*

Chair, Recruitment committee, Aalto University Department of Computer Science. (up to the long-listing stage) *2019*

Member, Recruitment committee, Aalto University Department of Computer Science. *2018*

Member, Tenure-track promotion committee, Aalto University School of Electrical Engineering (Department of Communications and Networking). *2018*

Member, Recruitment committee, Aalto University Department of Computer Science. *2017*

Chair, Recruitment committee, Aalto University School of Science (Department of Computer Science and Department of Mathematics & Systems Analysis). *2017*

Department representative, Tenure Track committee, Aalto University School of Science *2016-2019*

Research Area Representative, Department steering group, Aalto University Department of Computer Science. 2015-2016

Member, Recruitment committee, Aalto University School of Electrical Engineering (Department of Communications and Networking). *2014*

Department representative, Doctoral program committee, Aalto University School of Science. *2014-2019*

Member, Patent evaluation committee, Nokia. *2010-2012*

RESEARCH IMPACT

Here are three representative examples of different types of long-term impact (pioneering research, widespread impact, large-scale deployment) of my research. The paper numbers refer to the list in the Publications section.

- **Optimistic Fair Exchange (pioneering research)**: In my dissertation, I introduced the notion of *optimistic* fair exchange (Paper 10 and two companion papers). As a sensible middle ground between the two previously known approaches to fair exchange: using a trusted third party in every transaction or using expensive cryptographic protocols. The optimistic approach relied on an off-line trusted third party who needs to be invoked only if the exchange fails. This is an example of optimizing for the common case: the common case being situations where both parties in the exchange are honest and want to see the transaction completed. Our initial papers set off a flurry of research resulting in over 2400 citations to date in Google Scholar collectively for the three works.
- **Man-in-the-middle in Tunneled Authentication Protocols (widespread impact)**: In 2002, I and my collaborators discovered a flaw in composing two authentication protocols in different channels without properly binding them. Although the flaw is simple, at least in hindsight, it was widespread and occurred in many protocols that were being standardized by the Internet Engineering Task Force. Our paper (Paper 9) had wide-ranging impact in IETF ranging from the disbanding of the *IPSec remote access (ipsra)* and incorporating channel binding in a number of protocol specifications including popular ones like *IKEv2* and *PEAP*. Our work continues to have impact in the design of newer IETF protocols, for example as evidenced by the recently published IETF RFC 6813: *"The Network Endpoint Assessment (NEA) Asokan Attack Analysis"*, [2].
- **Secure First Connect (large scale deployment)**: In 2006, as part of the industry-wide effort to find more secure and more user-friendly solutions for the "First Connect" problem, my colleagues and I designed an efficient protocol for authenticating key agreement using short authenticated strings (US patent 7783041). The protocol was incorporated into the specifications of Bluetooth Special Interest Group and has been deployed in billions of devices that support Bluetooth versions 2.1 or later. (See Paper 7 for more information.)

I have also been working on a number of other system security topics during my career, including (most recent first):

Machine Learning vs. Security/Privacy Machine learning is transforming the landscape in many application scenarios. Security and privacy is no exception. My students and I have been applying machine learning for a variety of scenarios ranging from efficeintly detecting phishing websites, through detection of vulnerable IoT devices (Paper 3) to improving ease-of-use (See the paragraph on "contextual security" below). But it is also increasingly clear that in an adversarial setting, designers of machine learning applications have to take new security and privacy considerations into account. For example, we developed a technique called "MiniONN" to transform any existing cloud-hosted neural network to an oblvious form so that clients and servers can jointly compute neural network prediction without either party leaking sensitive information to the other party (Paper 4) and explored the threat of "model theft" and how to defend against it. Recently, we started investigating an important, but under-explored problem: how machine do learning defenses can affect *other unrelated risks* than the one they are meant to protect against (Paper 1) and how we can deploy multiple defenses simultaneously without such unintended interactions.

Hardware-assisted Protection: During the past fifteen years, my colleagues and I have been pioneering academic research work on hardware-assisted mechanisms for protecting software, especially on mobile devices (Paper 5). Our early work on "On-board Credentials (ObC)" (Paper 8) has been deployed in Nokia smartphone platforms. My students developed an opensource software framework called Open-TEE which allows developers to easily make use of mobile trusted computing. Open-TEE (IEEE TrustCom 2015) was covered by The Register[3]. The latest work

[2] http://tools.ietf.org/html/rfc6813

[3] http://www.theregister.co.uk/2015/06/30/opentee_an_open_virtual_trusted_execution_environment/

in this line of research shows how to use the new "pointer authentication" primitives in ARM processors to protect function returns (Paper 2).

Contextual Security: For security and privacy mechanisms intended for end users, a fundamental challenge is their (lack of) usability. One of my recent research directions is to investigate how the wealth of contextual information on mobile devices (such as data gathered by on-board sensors or interactions within social networks) can be used to improve usability without sacrificing security. Results of this work have appeared in various venues including IEEE PerCom 2011 (Best Demo Award) and 2014, ACM ASIACCS 2014 (Best Paper Award), ACM CCS 2014 and NDSS 2016.

Mobile Security: A consistent research theme in my work has been to study the security of mobile devices and mobile communication systems. This work ranged from analyzing mobile platform security (WWW 2012) and communication security architectures (NDSS 2016), designing new ways to use mobile security infrastructures (such as the work on Generic Authentication Architecture (GAA) described in the book on GAA I wrote with my colleagues "Cellular Authentication for Mobile and Internet Services [4]) to investigating the extent of mobile malware infection (Paper 6), which received wide press coverage, including by MIT Technology Review[5].

Security for Ad hoc Networking: Early in my career I worked on securing routing protocols for mobile ad hoc networks (ACM WiSe 2002, 1200+ citations) and the challenge of establishing ad hoc security associations between devices that have no prior context (Computer Communications, 23:17, pp 1627-1637, over 670 citations). The latter work paved the way for subsequent work on Secure First Connect discussed above.

FULL LIST OF SUCCESSFUL TECHNOLOGY TRANSFERS

Intel: An internal group at Intel has integrated our WAFFLE (Watermarking for Federated learning) technique, that I published in a paper with my student Buse Gul Atli Tekgul, into their OpenVINO system. *2022*

Nokia Research Center: Contributed to several research projects that led to successful technology transfers:

- Conceived, initiated, led and jointly designed protocols and architecture for the On-board Credentials technology (available on Nokia Symbian^3 and Windows Phone 8 devices) *2005-2012*
- Conceived, jointly initiated and designed protocols for the Magic Wand project which was eventually incorporated into various standards like Bluetooth Secure Simple Pairing (available on all devices supporting Bluetooth 2.1 or later) and Wireless USB Association Models *2003-2007*
- Conceived, jointly initiated and did initial groundwork on the GAIN project which developed the technology that eventually became standardized as Generic Authentication Architecture (deployed in Symbian OS GBA module as well as in Nokia Bootstrapping Server Function (BSF)) *2001-2006*
- Conceived, initiated, and initially led the MyPocket project which developed a remote storage framework for Symbian (which was eventually productized as the "remote storage" feature in Symbian^1 and Symbian^3 devices) 2003-2004
- Contributed to the design of Baseband-5 security architecture (deployed on most Nokia devices) *2000-2001*
- Jointly initiated the platform security research program B-Secure at Nokia Research Center (the program contributed to the design of Symbian OS platform security) *1999-2001*

[4] Wiley 2008 http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470723173.html

[5] http://www.technologyreview.com/view/522771/first-direct-measurement-of-infection-rates-for-smartphone-viruses/

IBM Research: Designed and implemented the Electronic Payment Service in the EU Project SEMPER which was transferred to IBM E-Till product group *1998*

RESEARCH AREAS

Systems Security and Privacy: for mobile and embedded devices, platform security, machine learning & security, secure communications, usable security, applied cryptography, secure electronic commerce.

Secure Distributed Systems: Blockchains and consensus, operating systems, mobile computing infrastructures, Internet-of-Things, IP networks, ad-hoc networks.

CITATION RECORD

- Google Scholar: `http://scholar.google.com/citations?user=0MqQ8AgAAAAJ` (**h-index: 77**)
- ACM Author: `http://dl.acm.org/author_page.cfm?id=81100611941`
- Web of Science: `https://www.webofscience.com/wos/author/record/150583` (**h-index: 34**)
- ORCID: `https://orcid.org/0000-0002-5093-9871`

SUMMARY OF PUBLICATION RECORD

(Note: Full publication record available at `https://asokan.org/asokan/profile/`)

- **Refereed Publications**:
  - 33 Papers in peer-reviewed international journals and magazines
  - 1 Survey article in an international technology magazine
  - 139 Papers in international conferences or workshops
  - 6 Book chapters
- **Unrefereed Publications**:
  - 8 Invited papers in international conferences or workshops
  - 3 Books
  - 104 Technical reports

MOST IMPORTANT PUBLICATIONS

1. Vasisht Duddu, Sebastian Szyller, N. Asokan: **SoK: Unintended Interactions among Machine Learning Defenses and Risks**. IEEE Symposium on Security & Privacy, May 2024: 2996-3014. https://doi.org/10.1109/SP54263.2024.00243 (**Distinguished Paper Award**)

2. Hans Liljestrand, Thomas Nyman, Lachlan J. Gunn, Jan-Erik Ekberg, N. Asokan: **PACStack: an Authenticated Call Stack** Usenix Security 2021. https://www.usenix.org/conference/usenixsecurity21/presentation/liljestrand

3. Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, Sasu Tarkoma: **IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT**. IEEE ICDCS 2017: 2177-2184, Atlanta, GA, June 2017, https://doi.org/10.1109/ICDCS.2017.283 (**Best Demo Award**)

4. Jian Liu, Mika Juuti, Yao Lu, N. Asokan: **Oblivious Neural Network Predictions via MiniONN transformations**, Proceedings of ACM Conference on Computer and Communication Security (ACM CCS), Dallas, November 2017. https://doi.org/10.1145/3133956.3134056 (Full version available as IACR ePrint report 2017/452, May 2015. https://eprint.iacr.org/2017/452)

5. N. Asokan, Jan-Erik Ekberg, Kari Kostiainen, Anand Rajan, Carlos V. Rozas, Ahmad-Reza Sadeghi, Steffen Schulz, Christian Wachsmann: **Mobile Trusted Computing**, Proceedings of the IEEE 102(8): 1189-1206 (2014). http://dx.doi.org/10.1109/JPROC.2014.2332007

6. Hien Thi Thu Truong, Eemil Lagerspetz, Petteri Nurmi, Adam Oliner, Sasu Tarkoma, N. Asokan, Sourav Bhattacharya: **The Company You Keep: Mobile Malware Infection Rates and Inexpensive Risk Indicators**, Proceedings of the 23rd International World Wide Web Conference (WWW 2014), Seoul, Korea, April 2014. http://doi.acm.org/10.1145/2566486.2568046 (Full version available as CoRR abs/1312.3245, December 2013. http://arxiv.org/abs/1312.3245)

7. Jani Suomalainen, Jukka Valkonen, N. Asokan: **(Standards for) Security Associations in Personal Networks: A Comparative Analysis**, in International Journal of Security and Networks (IJSN), special issue on "Secure Spontaneous Interaction", 2009. http://dx.doi.org/10.1504/IJSN.2009.023428

8. Kari Kostiainen, Jan-Erik Ekberg, N. Asokan Aarne Rantala: **On-board Credentials with Open Provisioning**, In Proceedings of the ACM ASIACCS conference, March 2009. http://doi.acm.org/10.1145/1533057.1533074 (earlier version available as Nokia Research Center Technical Report, NRC-TR-2008-007, August 2008. https://www.researchgate.net/publication/221609486_NRC-TR-2008-007_On-board_Credentials_with_Open_Provisioning

9. N. Asokan, Kaisa Nyberg, Valtteri Niemi: **Man-in-the-middle in Tunneled Authentication Protocols**, In Proceedings of the Eleventh International Security Protocols Workshop, volume 3364 of Lecture Notes in Computer Science, pages 28-41, April 2003, Springer. http://dx.doi.org/10.1007/11542322_6

10. N. Asokan, Victor Shoup, Michael Waidner: **Asynchronous Protocols for Optimistic Fair Exchange**

    In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA, May 1998. IEEE Computer Society Press, pages 86-99. http://dx.doi.org/10.1109/SECPRI.1998.674826

ROYALTY AWARDS

Nokia gives royalty awards for patents that have been incorporated into Nokia product(s) and have significantly improved the competitiveness of those products, for example by being deemed essential for implementing a standard specification the Nokia IPR department.

1. Method and apparatus for providing bootstrapping procedures in a communication network (US 9,300,641)
2. System and method for establishing bearer-independent and secure connections (US 8,484,466)
3. Requesting digital certificates (US 8,397,060)
4. Secure data transfer (US 8,145,907)
5. Method and system for managing cryptographic keys (EP 1561299, US 7,920,706)
6. System, method and computer program product for authenticating a data agreement between network entities (US 7,783,041)
7. Linked authentication protocols (US 7,707,412)
8. Authentication in a packet data network. (US 7,107,620, US 7,512,796, EP1273128)
9. System and method of bootstrapping a temporary public-key infrastructure from a cellular communication authentication and billing infrastructure. (US 7,107,248, EP1397787B1)
10. Address acquisition. (EP 1252781, US 6,959,009, US 7,920,575)

OTHER PATENTS

11. Method and system for byzantine fault-tolerance replicating of data (US 10,797,877)
12. Method and system for byzantine fault-tolerance replicating of data on a plurality of servers (US 10,664,353)
13. Implementation of an integrity-protected secure storage (US 10,565,400)
14. Method and device for verifying the integrity of platform software of an electronic device (US 10,482,238, 11,126,710)
15. Method and apparatus for identity based ticketing (US 10,374,799)
16. Method and system for byzantine fault-tolerance replicating of data on a plurality of servers (US 10,049,017)
17. Method and apparatus for accelerated authentication (US 9,979,545)
18. Method and apparatus for providing bootstrapping procedures in a communication network (US 9,906,528)
19. Method and device for verifying the integrity of platform software of an electronic device (US 9,881,150)
20. Device to device security using NAF key (US 9,781,085)
21. Mechanisms for certificate revocation status verification on constrained devices (US 9,756,036)
22. Method and apparatus for accelerated authentication (US 9,667,423)

23. Authenticating security parameters (US 9,503,462)
24. Method and device for verifying the integrity of platform software of an electronic device (US 9,438,608)
25. Implementation of an integrity-protected secure storage (US 9,171,187)
26. Method and apparatus to reset platform configuration register in mobile trusted module (US 9,087,198)
27. Methods and apparatus for reliable and privacy protecting identification of parties' mutual friends and common interests (US 9,003,486)
28. Method and device for verifying the integrity of platform software of an electronic device (US 8,954,738)
29. Method and apparatus for adjusting context-based factors for selecting a security policy (US 8,898,793)
30. Methods, apparatuses, and computer program products for bootstrapping device and user authentication (US 8,869,252)
31. Securing communication (US 8,769,284)
32. Credential provisioning (US 8,724,819)
33. Method, apparatus and computer program product for secure software installation (US 8,701,197)
34. Method and apparatus for selecting a security policy (US 8,621,656)
35. Method and apparatus to bind a key to a namespace (US 8,566,910)
36. Administration of wireless local area networks (US 8,532,304)
37. Authenticated group key agreement in groups such as ad-hoc scenarios (US 8,386,782)
38. Methods, apparatuses, and computer program products for authentication of fragments using hash trees (US 8,352,737)
39. Establishment of a trusted relationship between unknown communication parties (US 8,132,005)
40. Accessing protected data on network storage from multiple devices (US 8,059,818)
41. Method for remote message attestation in a communication system (US 7,913,086)
42. Information hiding non-interactive proofs-of-work (Korea 37764-KR-PCT)
43. Method for protecting electronic device, and electronic device (US 7,630,495)
44. System and method for dynamically enforcing digital rights management rules (US 7,529,929)
45. Secure backup and recovery using a key recovery service (Korea 808654)
46. Controlling delivery of certificates in a mobile communication system (US 7,526,642)
47. Method for sharing the authorization to use specific resources (US 7,343,014)
48. System and method of secure authentication and billing for goods and services using a cellular telecommunication and an authorization infrastructure (US 7,308,431)
49. Method, system, and devices for transferring accounting information (US 7,251,733)

50. Method, system and computer program product for secure ticketing in a communication device (US 7,207,060)
51. Method for applying electronic payment schemes in short-range e-commerce. (US 7,194,438)
52. IP mobility in a communication system (US 7,191,226)
53. Method, system and computer program product for a trusted counter in an external security element for securing a personal communication device. (US 7,178,041)
54. Personal device, terminal, server and methods for establishing a trustworthy connection between a user and a terminal (US 7,149,895, EP 1026641)
55. Addressing and routing in mobile ad hoc networks.
56. SIM based authentication mechanism for DHCPv4/v6 messages. (US 6,704,789, EP1175765B1)

EXTERNAL PRESENTATIONS

1. *Meta Concerns in ML security/privacy* (Invited keynote), The Second Symposium on Digital Trust, Digital Trust Centre, Nanyang Technological University, Singapore. February 2025.
2. *Meta Concerns in ML security/privacy* (Invited research talk), Linköpings universitet, Sweden. November 2024.
3. *Confidence in AI: Can we trust AI-based systems?* (Invited research talk), Ericsson, Sweden. November 2024.
4. *Confidence in AI: Can we trust AI-based systems?* (Invited research talk), Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi Selangor, Malaysia. October 2024.
5. *Model Stealing Attacks and Defenses: Where Are We Now?* (Invited talk), CS Seminar, City University of Hongkong, Hong Kong. September 2024.
6. *Confidence in AI: Can we trust AI-based systems?* (**Invited keynote**), Secure and Scalable Machine Learning Symposium, VISTEC, Rayong, Thailand. August 2024.
7. *Confidence in AI: Can we trust AI-based systems?* (Invited lecture), FSKTM, Universiti Malaya, Kuala Lumpur, Malaysia. August 2024
8. *Blinded Memory*, (Invited talk), Institut d'informatique, Université de Neuchâtel, Neuchâtel, Switzerland. June 2024.
9. *Blinded Memory*, (Invited talk), KTH Security Seminar (Invited talk), Stockholm, Sweden . May 2024.
10. *Blinded Memory*, (Invited talk), ETH CS Distinguished Colloquium, Zürich, Switzerland. May 2024.
11. *Model Stealing Attacks and Defenses: Where Are We Now?* (Invited seminar), Cybersecurity and Privacy (CySeP) Summer School, Stockholm, Sweden. June 2024.
12. *Model Stealing Attacks and Defenses: Where Are We Now?* (Invited talk), IBM Research Europe – Zurich, Rüschlikon, Switzerland. June 2024
13. *Model Stealing Attacks and Defenses: Where Are We Now?* (Invited talk), Cryptology and Data Security Group, Institute of Computer Science, University of Bern, Bern, Switzerland. June 2024.
14. *Model Stealing Attacks and Defenses: Where Are We Now?* (Invited talk), ZISC Seminar, Zurich Information Security/Privacy Center, ETH, Zürich, Switzerland. April 2024.
15. *Model Stealing Attacks and Defenses: Where Are We Now?*, (Invited talk) at School of Electrical Engineering and Computer Science, KTH, Stockholm, Sweden. January 2024
16. *Real-world (Cyber)Security with Kaisa Nyberg: A Personal Perspective*, (Invited talk) at Aalto University, Finland. October 2023
17. *Model Stealing Attacks and Defenses: Where Are We Now?*, (Invited talk) at Department of Computer Engineering, Chiang Mai University, Chiang Mai, Thailand. July 2023
18. *Model Stealing Attacks and Defenses: Where Are We Now?*, (**Invited keynote**) at ASIACCS 2023, Melbourne, Australia. July 2023

19. *Model Stealing Attacks and Defenses: Where Are We Now?*, (Guest lecture) at Universiti Tunku Abdul Rahman, Kampar, Malaysia. July 2023

20. *Model Stealing Attacks and Defenses: Where Are We Now?*, (Guest lecture) at IT Bandung, Bandung, Indonesia. July 2023

21. *Blinded Memory*, Invited talk, Concordia University, Montreal, Canada. June 2023

22. *Blinded Memory*, Invited talk, German University of Cairo, Cairo, Egypt. May 2023

23. *Extraction of Complex DNN Models: Real Threat or Boogeyman?*, Invited talk, KAUST, Thuwal, Saudi Arabia. May 2023

24. *False Claims Against Model Ownership Resolution*, Invited talk, Rochester Institute of Technology, Rochester, USA. May 2023

25. *False Claims Against Model Ownership Resolution*, Invited talk, Intel Labs, Portland, USA. May 2023

26. *Model Stealing Attacks and Defenses: Where Are We Now?*, (Invited talk) at Reed College, Portland, USA. May 2023

27. *Technology Transfer from Security Research Projects: A Personal Perspective*, (**Invited keynote**) at ICISS 2022, Virtual (Tirupati), India. Dec 2022

28. *Confidence in AI systems: Can we trust AI-based systems?*, (**Invited keynote**) at the Industry Summit at the Conference on Privacy, Security & Trust, Fredericton, New Brunswick, Canada. August 2022

29. *Extraction of Complex DNN Models: Real Threat or Boogeyman?*, (**Invited keynote**) at Conference on Privacy, Security & Trust, Fredericton, New Brunswick, Canada. August 2022

30. *Confidence in AI systems: Can we trust AI-based systems?*, (Invited talk) at Hack Your Tomorrow hackathon, Project Tech Conferences, Virtual, Canada. August 2022

31. *Hardware-assisted Run-time Protection: on balancing security and deployability*, (Invited talk) at the OpenS3 Lab workshop on "Building Intelligent Trustworthy Computing Systems: Challenges and Opportunities", Virtual (Darmstadt), Germany. November 2021

32. *Confidence in AI systems: Can we trust AI-based systems?*, (Invited talk) at International Conference of Governance on Digital Technology, Zhejiang University, Virtual (Beijing), China. June 2022

33. *Confidence in AI systems: Can we trust AI-based systems?*, (Invited talk) at Techtalk, IEEE Student Branch, University of Jaffna, Virtual (Jaffna), Sri Lanka. February 2021.

34. *Confidence in AI systems: Can we trust AI-based systems?*, (Invited talk) at AI Industry Day, University of Waterloo AI Institute, Virtual (Waterloo), Canada. March 2021.

35. *Confidence in AI systems: Can we trust AI-based systems?*, (Invited talk) at Waterloo.AI Reverse Co-op, University of Waterloo AI Institute, Virtual (Waterloo), Canada. June 2021.

36. *Extraction of Complex DNN Models: Real Threat or Boogeyman?*, (**Invited keynote**) at IEEE Conference on Communications and Network Security. October 2021

37. *Hardware-assisted Run-time Protection: on balancing security and deployability*, (Invited talk) at Hot Issues in Security Principles and Trust (HotSpot 2021), Virtual (Vienna), Austria. September 2021

38. *Hardware-assisted Run-time Protection: on balancing security and deployability*, (Invited talk) at the Public Lecture Series, Univerasity of Toronto, Identity, Privacy, and Security Institute, Virtual (Toronto), Canada. April 2021

39. *Extraction of Complex DNN Models: Real Threat or Boogeyman?*, (Invited talk) at CASA Distinguished Lecture Series, Ruhr University of Bochum, Bochum, Germany. November 2020

40. *Extraction of Complex DNN Models: Real Threat or Boogeyman?*, (Invited talk) at Huawei Helsinki Cloud Service Summit 2020, Helsinki, Finland. November 2020

41. *Hardware-assisted Run-time Protection*, (Invited lecture) at Zhejiang University School of Cyber Science and Technology Overseas lectures, Hangzhou, China May 2020, August 2021

42. *Security, Privacy, and Machine Learning*, (Invited talk) at Asian Institute of Technology, Bangkok, Thailand. January 2020

43. *Trustworthy and Accountable Function-as-a-Service*, (**Invited keynote**), OWASP Thailand DevSecOps in Action Conference, Bangkok, Thailand. January 2020

44. *Hardware-assisted Trusted Execution Environments* (**Invited keynote**), at 2019 Westlake International Forum, Hangzhou, China. November 2019

45. *Hardware-assisted Trusted Execution Environments* (**Invited keynote**), at ACM CCS 2019, London, UK. November 2019

46. *Hardware-assisted Trusted Execution Environments* (Invited keynote), at Virgina Tech Distinguished Lecture, Blacksburg, USA. November 2019

47. *Securing cloud-assisted Services* (Invited talk), at Uber HQ, San Francisco, USA. June 2019

48. *The Undeniable Truth: How Remote Attestation Circumvents Deniability Guarantees in Secure Messaging Protocols* (Invited talk), at the 2600 Thailand Red Pill Blue Pill Security Conference, Bangkok, Thailand. May 2019

49. *Securing cloud-assisted services* (Invited talk), at the annual Huawei Science and Technology Workshop, Shenzhen, China. May 2019

50. *Hardware-assisted run-time Protection* (Invited talk), at CRISP Distinguished Lecture Series, TU Darmstadt, Germany. February 2019

51. *Common-sense Applications of Hardware-based Trusted Execution Environments* (Invited talk), International Workshop on Banking Security with Trusted Hardware , Bangkok, Thailand. December 2018

52. *The Undeniable Truth: How Remote Attestation Circumvents Deniability Guarantees in Secure Messaging Protocols* (Briefing), at BlackHat EU, London, UK. December 2018

53. *Hardware-assisted run-time Protection* (Invited talk), at Google Android Security Local Research Day (ASLR-D), Mountain View, USA. October 2018

54. *Common-sense Applications of Hardware-based Trusted Execution Environments* (Invited talk), at Huawei Security and Privacy workshop, Helsinki, Finland. October 2018

55. *On secure resource accounting for outsourced computation* (Invited talk), at Sunblaze group, University of California, Berkeley, USA. October 2018

56. *Can Blockchains be made better using hardware-assisted security* (Invited talk), at the Blockchain Symposium, Center for Secure Distributed Ledgers and Contracts, Darmstadt, Germany. September 2018

57. *On secure resource accounting for outsourced computation* (**Invited keynote**), at SysTEX 2018, Toronto, Canada. October 2018

58. *Securing Cloud-assisted Services* (Invited talk), at School on Security & correctness in the Internet of Things, Graz, Austria. September 2018

59. *Securing Cloud-assisted Services* (Invited plenary talk), at CySeP summer school, KTH, Stockholm, Sweden. June 2018

60. *Machine Learning in the Presence of Adversaries* (Invited talk), at Nokia Bell Labs, Espoo, Finland. April 2018

61. *Machine Learning in the Presence of Adversaries* (Invited talk), at Shonan seminar on resilient machine-to-machine communication, Shonan, Japan. March 2018

62. *Common-sense Applications of Hardware-based Trusted Execution Environments* (Invited talk), at NYU Tandon School of Engineering, New York, NY, USA. March 2018

63. *Securing Cloud-assisted Services* (**Invited keynote**), at Data 61 Cyber Summer School, Melbourne, Australia February 2018

64. *Common-sense applications of hardware-based trusted execution environments* (**Invited keynote**), at the Workshop on Trusted Computing and its Applications, Surrey, UK. January 2018

65. *Securing Cloud-assisted Services* (Invited talk), at Secure Cloud Services and Storage Workshop, Oslo, Norway. September 2017

66. *Fast client-side phishing detection: a case-study in applying machine learning to solve security/privacy problems*, (Invited talk), CROSSING conference, TU Darmstadt, Germany. May 2017

67. *Securing Cloud-assisted Services* (Invited talk), at LORIA, Nancy, France. April 2017

68. *Fast client-side phishing detection*, (Invited talk), School of EEE, Nanyang Technological University, Singapore. April 2017

69. *Securing Cloud-assisted Services* (Invited talk), at NEC Labs, Tokyo, Japan. January 2017

70. *Technology Transfer from Security Research Projects: A Personal Perspective* (Invited talk), at NTT Mushahino R&D Center, Tokyo, Japan. January2017

71. *Securing Cloud-assisted Services* (**Invited keynote**), at the SECODIC workshop, Salzburg, Austria. September 2016

72. *How Far Removed Are You? Scalable Privacy-Preserving Estimation of Social Path Length* (Invited talk), at the International Summer School on Social Networks Security, Privacy, and Trust" (SNSPT), Padova, Italy. September 2016

73. *Things, Trouble, Trust: On Building Trust in IoT Systems* (Invited talk), at the CROSSING seminar, TU Darmstadt, Germany. August 2016

74. *The Quest for Usable Security* (Invited talk), University of Surrey workshop on Mobile Security, Surrey, UK. December 2015

75. *Technology Transfer from Security Research Projects: A Personal Perspective* (**Invited keynote**), at 20th Nordic IT Security Conference (NordSec), KTH, Stockholm, Sweden. October 2015

76. *The Quest for Usable Security* (Invited talk), Android Security Symposium, Vienna, Austria (video: `https://youtu.be/gVPkFV5Zg2c`) September 2015

77. *How Far Removed Are You? Scalable Privacy-Preserving Estimation of Social Path Length* (Invited talk) University of Oxford, Oxford, United Kingdom March 2015

78. *How Far Removed Are You? Scalable Privacy-Preserving Estimation of Social Path Length* (Invited talk) Security Seminar, University of Edinburgh, Edinburgh, United Kingdom January 2015

79. *On Mobile Malware* (Invited talk), School of Computer Science Colloquium, McGill University, Montréal, Canada. December 2014

80. *Technology Transfer from Security Research Projects: A Personal Perspective* (Invited lecture), at Cybersecurity and Privacy (CySeP) Winter School, KTH, Stockholm, Sweden. October 2014

81. *On Mobile Malware* (**Invited keynote**), ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Oxford, United Kingdom. July 2014

82. *On Mobile Malware* (Invited talk), NEC Labs Europe, Heidelberg, Germany. January 2014

83. *On Mobile Malware* (Invited talk), CrySP Speaker Series, University of Waterloo, Canada. (video: `https://crysp.uwaterloo.ca/events/20131216-Asokan.mp4`) December 2013

84. *The Untapped Potential of TEEs on Mobile Devices* (**Invited keynote**), Financial Cryptography and Data Security Conference (FC), Okinawa, Japan. April 2012

85. *Mobile Platform Security Architectures* (**Invited keynote**), 11th Smart Card Research and Advanced Application Conference (CARDIS), Graz, Austria. November 2012

86. *Context Profiling for Mobile Devices* (Invited talk), Securing Clouds & Mobility Track, Intel European Research & Innovation Conference (ERIC 12), Barcelona, Spain. October 2012

87. *The Case for Usable Mobile Security* (Invited talk), Department of Computer Science, University of Helsinki. August 2012

88. *Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling* (Invited), University of Colombo School of Computer Science (UCSC), University of Colombo, Sri Lanka. July 2012

89. *The Case for Usable Mobile Security* (**Invited Keynote**), Jaffna University International Research Conference (JUICE-2012), University of Jaffna, Sri Lanka. July 2012

90. *Solutions for Mobile Security and Privacy Protection* (**Invited Keynote**), Trust in Digital Life workshop, Biel, Switzerland. March 2012

91. *Intuitive security policy configuration in mobile devices using context profiling* (Invited Guest Talk), IIIT-Bangalore, India. February 2012

92. *Usable Mobile Security* (**Invited keynote**), 8th International Conference on Distributed Computing and Internet Technology (ICDCIT 2012), Bhubaneswar, India. February 2012

93. *On "Device Clouds"* (Invited participant talk), Dagstuhl 11491 "Secure Computing in the Cloud", Dagstuhl, Germany. December 2011

94. *Usable mobile security* (**Invited keynote**), First International Workshop on Trustworthy Embedded Devices, Leuven, Belgium. September 2011

95. *A Perspective on the Evolution of Mobile Platform Security Architectures*, (Invited) Laboratory for Communications and Applications, EPFL, Switzerland. April 2011

96. *A Perspective on the Evolution of Mobile Platform Security Architectures*, (Invited) ETH Zurich Computer Science Colloquium, Zurich, Switzerland. March 2011

97. *A Perspective on the Evolution of Mobile Platform Security Architectures* (**Invited keynote**), First ACM Conference on Data and Application Security and Privacy (ACM CODASPY), San Antonio, Texas, USA. February 2011

98. *On-board Credentials* (Invited), Electrical and Computer Engineering, University of Toronto, Canada. August 2010

99. *Intuitive and Sensible Access Control* (Invited), Security group, NTNU, Trondheim, Norway. January 2010

100. *On-board Credentials with Open Provisioning* (Invited), Q2S, NTNU, Trondheim, Norway. January 2010

101. *Discrimination is Useful: Why and How to discriminate messages in public DTNs* (Invited participant talk), Dagstuhl 09071 "Delay and Disruption-Tolerant Networking (DTN) II", Dagstuhl, Germany. February 2009

102. *On-board Credentials with Open Provisioning* (Invited), Distinguished Lecturer Seminar Series, Donald Bren School of Information and Computer Sciences, University of California, Irvine, California, USA. October 2008

103. *On-board Credentials with Open Provisioning* (**Invited keynote**) at the Workshop in Information Security Theory and Practices (WISTP) 2008, Seville, Spain. May 2008

104. *Securing Disruption-tolerant Communication*, (Invited), DIT seminar series, Dipartimento di Ingegneria e Scienza dell'Informazione - DISI, University of Trento, Italy. *February 2008*

105. *Securing Disruption-tolerant Communication*, (Invited), Computer Science Department, University of Calgary, Canada. *January 2008*

106. *Securing First Connect*, (Invited), Computer Science Department, University of Calgary, Canada. *January 2008*

107. *Identity-based Cryptography for Security in Disruption-prone Environments*, Internet Research Task Force, DTNRG working group meeting, Dublin, Ireland. *May 2007*

108. *Security Associations for Personal Devices*, (Invited) Horst Görtz Institute for IT-Security, Ruhr University of Bochum, Germany. *March 2007*

109. *Security Associations for Personal Devices*, (Invited) Networking Laboratory, Helsinki University of Technology, Finland. *February 2007*

110. *Security Associations for Personal Devices*, (Invited) IBM T.J. Watson Research Center, Hawthorne, NY, USA. *February 2007*

111. *Phishing and Phones*, (Invited) Panel on "Future of Phishing", Usable Security Workshop, Tobago. *February 2007*

112. *Securing First Connect*, (Invited) Distributed systems seminar, University of Waterloo, Canada. *May 2006*

113. *Issues in Initializing Security*, (Invited) IEEE Symposium on Signal Processing and Information Technology, Athens, Greece *December 2005*

114. *Man-in-the-middle in Tunnelled Authentication protocols*, Security Protocols Workshop, Cambridge, UK. *April 2003*

115. *Security Issues in Ad-hoc Routing Protocols* (Invited), École Polytechnique Fédérale de Lausanne, Switzerland. *December 2002*

116. *AAA for IPv6 network access*, (Invited) Faster Pro 2001 Workshop, Tampere University of Technology, Finland. *January 2001*

117. *New uses for the cellular authorization infrastructure*, Helsinki University of Technology, Finland. *December 2000*

118. *Fair Exchange*, University of Alberta, Canada. *May 2000*

119. *Fair Exchange*, University of Waterloo, Canada. *April 2000*

120. *Security Issues in Mobile Communication Systems*, (Invited) IETF Internet Architecture Board (IAB) workshop on wireless internetworking, Mountain View, CA., USA. *March 2000*

121. *Generic Electronic Payment Service*, 2^{nd} SEMPER day seminar, Zurich, Switzerland. *December 1998*

122. *Fairness in Electronic Commerce*, Public thesis defense, University of Waterloo, Canada. *May 1998*

123. *Asynchronous Protocols for Optimistic Fair Exchange*, IEEE Symposium on Security and Privacy, Oakland, CA., USA. *May 1998*

124. *Secure Electronic Commerce*, (Invited) 10th Prognose Zirkel Zürich Info Day, Technopark, Zurich, Switzerland. *March 1998*

125. *Secure Electronic Commerce*, Distributed systems seminar, University of Waterloo, Canada. *May 1997*

126. *Optimistic Fair Exchange*, ACM CCS '97, Zurich, Switzerland. *April 1997*

127. *Server Supported Signatures*, ESORICS '96, Rome, Italy. *September 1996*

128. *Anonymity in Mobile Computing Environments* (panel participant), MCSA '94 workshop, Santa Cruz, CA., USA. *December 1994*

129. *A Parallel Implementation of the Hough Transform Method*, 32nd Midwest Symposium on Circuits and Systems, Urbana-Champaign, IL., USA. *August 1989*