Global Initiative of Academic Network

(Faculty from outside India only can use this format)

Name of the Faculty: Prof. N. Asokan

Affiliation: Aalto University, Finland

Address: Mäntytie 22, 02270 Espoo, Finland

Contact No: +358 50 483 6465

Email: asokan@acm.org

Course Title: Mobile Systems Security

Broad Area: Systems Security

Overview:

Mobile devices and mobile communication have become pervasive and are intertwined with every aspect of the lives of ordinary people. The mobile device ecosystem has many stakeholders with different interests. These have led to a variety of software and hardware security mechanisms being designed and deployed widely in today's mobile device platforms. Several of the underlying concepts and techniques however date back to the early days of computing. This course will provide an introduction to mobile systems security to the participants by introducing them various system security aspects as well as specific case studies such as Android OS platform security, hardware security mechanisms like TrustZone and Trusted Platform Module. It will also expose participants to the hard challenges in the domain such as the importance of and difficulties in designing secure systems that are intuitive and easy-to-use.

Objectives:

The primary objectives of the course are as follows:

i) Exposing participants to the fundamentals of mobile systems security

ii) Enhancing the ability of the participants to recognize and appreciate design challenges in this area by discussing specific example systems in software and hardware mobile platform security

iii) Giving the participants a larger perspective by developing general models for software and hardware mobile platform security

iv) Introducing participants to some current research problems in mobile systems security

Tentative Dates fort he course:

One week: Nov 21-25, 2016
Course Schedule (19 Hours):

Lecture 1 (02 Hours) This lecture will introduce the objectives of the course module and basic concepts. We will cover the basics of access control and examples of access control models. We will conclude with a historical background of mobile platform security and why it differs from platform security in traditional personal computers.

Lecture 2 (02 Hours) This lecture will provide an in-depth look at Android as a software platform focussing on the various platform security techniques used in Android.

Exercise session 1 (02 Hours) The first exercise session will cover three written exercises involving access control and Android platform security. During the first hour students will independently work on the exercises. The second hour will be structured as a discussion session where selected students will present their answers, followed by a discussion in the class as a whole.

Lecture 3 (03 Hours) This lecture will take a step back and develop an informal general models for platform security. We will start with an informal general model for software platform security leveraging the concepts learned in Lecture 2. We will then identify desirable hardware security features that can strengthen software platform security. Finally we will proceed to build an informal general model for hardware platform security including trusted execution environments (TEEs)

Lecture 4 (03 Hours) This lecture will begin with a recap of the general model for hardware platform security and go on to focus on two specific example TEEs. We will briefly discuss TrustZone and discuss efforts at making hardware platform security features in smartphones accessible to application developers, including the TEE interfaces being standardized by GlobalPlatform. We will then discuss trusted computing concepts introduced by the Trusted Computing Group (TCG), including the Trusted Platform Module (TPM). Finally we will take an in-depth look at the concepts underpinning TPM-2 Extended Authorization.

Exercise session 2 (02 Hours) The second exercise session will cover three written exercises involving TPM-2 Extended Authorization. During the first hour students will independently work on the exercises. The second hour will be structured as a discussion session where selected students will present their answers, followed by a discussion in the class as a whole.

Lecture 5 (02 Hours) This lecture will cover the usability challenges of mobile systems security. We will begin with the usability considerations of permission granting in smartphone platforms. We will then look at other system security problems that require balancing security and usability.

Exercise session 3 (02 Hours) The final exercise session will cover three written exercises involving usability of security mechanisms. . During the first hour students will independently work on the exercises. The second hour will be structured as a discussion session where selected students will present their answers, followed by a discussion in the class as a whole.

Lecture 6 (01 Hours) In the final lecture, we will recap what we learned in the course module and then go on to discuss some recent research and open problems in mobile systems security.

Who can attend

- Executives, engineers and researchers industry and government organizations including R&D laboratories interested in understanding mobile systems security

- Student students at advanced undergraduate (BTech 3rd/4th year) or graduate level /MSc/MTech/PhD) or Faculty from reputed academic institutions and technical institutions, especially those that want to do research in mobile systems security

The course will assume that the participant has already taken an undergraduate level coruse in security and cryptography or the equivalent. In particular, knowledge of basic cryptography and security techniques will be assumed.

Registration Fees

Participants from abroad	:	US $100
Industry/ Research Organizations:	:	Rs. 5000/-
Faculty members from Academic Institutions	:	Rs. 2500/-
Research Scholars/Postgraduate students	:	Rs 1000/-
Faculty/Research Scholars/Postgraduate students (MNIT)	:	NIL
Undergraduate students (in final year) (MNIT)	:	NIL

The above fee includes all instructional materials, computer use for tutorials and free Internet facility. The participants will be provided with accommodation, if available, on payment basis.

Supplementary Reading for Course Module:

1. N.Asokan, Lucas Davi, A. Dmitrienko, S.Heuser et. al.: Mobile Platform Security, Morgan and Claypool Publishers, Synthesis Lectures, 2014. Available at http://www.morganclaypool.com/doi/abs/10.2200/S00555ED1V01Y201312SPT009 for institutions with subscription.
2. Kari Kostiainen, Elena Reshetova, Jan-Erik Ekberg, N. Asokan: Old, new, borrowed, blue --: a perspective on the evolution of mobile platform security architectures. ACM CODASPY 2011: 13-24. **Freely available** courtesy ACM Author'ize by going via the author home page at http://asokan.org/asokan/research/
3. Brian McGillion, Tanel Dettenborn, Thomas Nyman, N. Asokan: Open-TEE - An Open Virtual Trusted Execution Environment. TrustCom/BigDataSE/ISPA (1) 2015: 400-407. **Freely available** at http://arxiv.org/abs/1506.07367
4. Thomas Nyman, Jan-Erik Ekberg, N. Asokan: Citizen Electronic Identities using TPM 2.0. TrustED@CCS 2014: 37-48. **Freely available** either at http://arxiv.org/abs/1409.1023 or (courtesy ACM Author'ize) by going via the author home page at http://asokan.org/asokan/research/
5. Jan-Erik Ekberg, Kari Kostiainen, N. Asokan: The Untapped Potential of Trusted Execution Environments on Mobile Devices. IEEE Security & Privacy 12(4): 29-37 (2014). Available at http://dx.doi.org/10.1109/MSP.2014.38 for IEEEXplore subscribers)
6. 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). **Freely available** at http://dx.doi.org/10.1109/JPROC.2014.2332007
7. Kari Kostiainen, Jan-Erik Ekberg, N. Asokan, Aarne Rantala: On-board credentials with open provisioning. ASIACCS 2009: 104-115. . **Freely available** courtesy ACM Author'ize by going via the author home page at http://asokan.org/asokan/research/

Proposed Budget:

S.No	Description of budgetary head	Amount (Rs.)
1.	(a) Air Fare (International Expert) (b) Honorarium to Expert	3,70,000[1]
2.	Lecture Notes material preparation	2,00,000[2]
3.	Contingency (Boarding and lodging at MNIT guest house**, Visa fee, etc.)	75,000
4.	Miscellaneous expenditure (including of Video recording expenses, if any) (Item 1 to 4 should not exceed 12000 USD)	75,000
5.	Host Faculty and/or Coordinator Honorarium*	
	GRAND TOTAL	**7,20,000**

* Honorarium to course coordinator should be paid from the registrations received from the participants.

** In case of unavailability of the guest house, accommodation in an economy hotel as per provisions of 6CPC shall be arranged.

Course Coordinators:

1. Dr. Manoj Singh Gaur
Professor
Department of Computer Science and Engineering
Malaviya National Institute of Technology Jaipur
JLN Marg, Jaipur – 302017, India.
Tel: +91-141-2713227 (O), +91-141-2713127 (R), +91 9414045867 (M)
Email: gaurms@mnit.ac.in

2. Dr. (Mrs.) Vijay Laxmi
Associate Professor
Department of Computer Science and Engineering
Malaviya National Institute of Technology Jaipur
JLN Marg, Jaipur – 302017, India.
Tel: +91-141-2713333 (O), +91-141-2713127 (R), +91 96807901204 (M)
Email: vlaxmi@mnit.ac.in

Foreign Teaching Faculty

Prof. N. Asokan is a Professor of Computer Science at Aalto University and the University of Helsinki.

Between 1995 and 2012, he worked in industrial research laboratories designing and building secure systems, first at the IBM Zurich Research Laboratory and then at Nokia Research Center. His primary research interest has been in applying cryptographic techniques to design secure protocols for distributed systems. Recently, he has also been investigating the use of Trusted Computing technologies for securing endnodes, and ways to make secure systems usable, especially in the context of mobile devices. Asokan is a co-author of over 80 research papers in international conferences and journals. He is a co-inventor of 41 granted patents. Asokan and his group pioneered early academic research involving trusted execution environments (TEEs) in mobile devices with their work on On-board Credentials.

Asokan serves on the editorial board of IEEE Security & Privacy and the Proceedings of Privacy Enhancing Technologies (PoPETS). He has previously served on the editorial boards of ACM Transactions on Information and Systems Security, Computer Communications, and IEEE Network and on the steering committees of ACM WiSec and ACM SPSM. His research has won best paper and best demo awards in venues such as ACM ASIACCS and IEEE PerCom. In 2013, he was selected for a Google Faculty Research Award for his work on contextual security.

Asokan received his doctorate in Computer Science from the University of Waterloo, MS in Computer and Information Science from Syracuse University, and BTech (Hons.) in Computer Science and Engineering from the Indian Institute of Technology at Kharagpur. He is an ACM Distinguished Scientist and an IEEE Senior Member.

For more information about Asokan's work see his website at http://asokan.org/asokan

PROF. N. ASOKAN

PERSONAL INFORMATION

E-mail: asokan@acm.org,asokan@ieee.org

Address: Mäntytie 22, 02270 Espoo, Finland.

Phone: +358 50 483 6465; *Website:* http://asokan.org/asokan/

Nationality: Citizen of Canada; Permanent resident of 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

Aalto University, Finland. *From August 2013*

Professor (tenured), *Department of Computer Science.*

PREVIOUS WORK EXPERIENCE

University of Helsinki, Finland. *September 2012 - July 2016*

Professor, *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.*

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:

Aalto University and University of Helsinki

System Security: mobile platform security, 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.
Collaborative project: Participation in European Commission fifth framework project *CyberVote*.

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.

Collaborative project: Participation in European Commission ACTS project *SEMPER*.

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.

Research Leadership:

Aalto University

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

Leading projects: Lead Academic Principal Investigator, ICRI-SC (2014-); Technical leadership of two Academy of Finland projects (CloSe and ConSec).

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-).

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

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

€280 011: PI, "Cloud Security Services" (CloSe), *Academy of Finland* *2014-2016*

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

€400 000: Lead PI, *Intel Collaborative Research Institute for Secure Computing* (ICRI-SC) at Aalto University *2014-2016*

US $50 000: 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*

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. Andrew Paverd, Aalto University *2015-*
2. Dr. Samuel Marchal, Aalto University *2015-*
3. Dr. Ravishankar Borgaonkar, Aalto University *2015*
4. Dr. Hien Truong, University of Helsinki *2013-2016*
5. Dr. Sourav Bhattacharya, Aalto University (now at Bell Labs) *2014*
6. Dr. Sini Ruohomaa, University of Helsinki (now at Ericsson) *2013-2014*

Supervision of doctoral research:

1. *Mika Juuti* *In progress*

2. *Thomas Nyman* *In progress*
3. *Jian Liu* *In progress*
4. *Elena Reshetova* *In progress*
5. *Sandeep Tamrakar* *In progress*

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

1. *Jan-Erik Ekberg*, "Securing Software Architectures for Trusted Processor Environments", Aalto University. (Director of Advanced Development, Trustonic Inc.) *2013*
2. *Kari Kostiainen*, "On-board Credentials: An Open Credential Platform for Mobile Devices", Aalto University. *Accepted with distinction ('kiittäen hyvksytty')*. (Postdoc., ETH Zürich) *2012*

Supervisor: MSc theses:

(as Professor at Aalto University)

1. *Pävivi Tynninen*, *2016*
2. *Kalle Saari*, *2016*
3. *Lari Lehtomäki*, *2016*
4. *Setareh Roshan Kokabha*, "An Online Anomaly-Detection Neural Networks-based Clustering for Adaptive Intrusion Detection Systems" *2016*
5. *Swapnil Udar*, "Contextual Authentication and Autho- rization using Wearable Devices". *2016*
6. *Nguyen Hoang Long*, "Securely accessing encrypted cloud stor- age from multiple devices" *2015*
7. *Robin Babujee Jerome*, "Pre-processing Techniques for Anomaly Detection in Telecommunication Networks". *2015*

(as Professor at University of Helsinki)

8. *Jian Liu*, "How to Steer Users Away from Unsafe Content". *2014*
9. *Xiang Gao*, "Strengthening Zero-Interaction Authentication Using Contextual Co-presence Detection". *2014*
10. *Thomas Nyman*, "Dynamic Isolated Domains". *2014*

(as Professor at Helsinki University of Technology)

11. *Pekka Sillanpää*, "Distributed Digital Identity System – Peer-to-Peer Perspective". *2007*
12. *Aishvarya Sharma*, "On-board Credentials: Hardware assisted secure storage of credentials". *2007*
13. *Cherdpan Sripan*, "User-to-Service authentication Using Mobile phones". *2006*
14. *Antti Halla*, "Applying a Systems Approach to Security in a Voice Over IP System". *2006*
15. *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 research interns: These interns typically spent 4-6 months in my group 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 (or is planned to be) 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:

Aalto University

Mobile System Security. *Spring 2015,2016*

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

Three lectures sponsored by the 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 Platform Security. *Spring 2014*

Teaching – tutorials:

1. *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*
2. *Mobile Security*, Three lectures at the **International Summer School on Information Security**, Bilbao, Spain, `http://grammars.grlmc.com/InfoSec2015/` *July 2015*
3. *Mobile Security*, Three 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*
4. *Mobile Security*, Two 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*
5. *Mobile Platform Security Architectures*, Half day tutorial, **International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2012)**, Indian Institute of Technology, Chennai, India, `http://space.cse.iitm.ac.in/Workshops.html` *October 2012*
6. *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, `http://space.cse.iitm.ac.in/Workshops.html` *October 2012*
7. *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
8. *Initializing Security Associations for Personal Devices*, **ZISC workshop on Wireless Security**, ETH Zürich, Switzerland. *September 2007*

AWARDS AND HONOURS

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. (`http://research.google.com/university/relations/fra_recipients.html`) *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:

IEEE *Security and Privacy*. *2016-*
Associate Editor, ACM Transactions on Information and System Security (TISSEC) *2013-2016*
Proceedings on Privacy Enhancing Technologies (PoPETs). *2014-2015*
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM). *2013-*
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:

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*

[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.

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 Symposium on Information, Computer and Communications Security (ACM ASIACCS). *2008-2010, 2015*

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:

Nokia and CE4A: Terminal Mode (later “MiirorLink”)Technical Architecture v1.0. *2010*

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*

Dissertation committees/Dissertation examinations:

Doctoral level: Claudio Marforio (ETH Zürich, December 2015), Guillermo Suárez.Tabgil (Universidad Carlos III de Madrid, October 2014), Nils Ole Tippenhauer (ETH Zürich, March 2012), Ersin Uzun and John Solis (University of California at Irvine, August 2010), Levente Buttyán, (École Polytechnique Fédérale de Lausanne, July 2002), Tuomas Aura (Helsinki University of Technology, November 2000).

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

Invited Service in Expert Groups:

Expert evaluator, EU program (details to be disclosed after evaluation is completed). *2016*

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:

Research Area Representative, Department Gteering Group, Aalto University Department of Computer Science. 2015-

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

Department representative, Doctoral Program Committee, Aalto University School of Science. *2014-*

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 the late 1990s, 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 1500 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 hundreds of millions of devices that support Bluetooth versions 2.1 or later. (See Paper 7 for more information.)

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

I have worked on a number of other system security topics during my career, including:

Security for Ad hoc Networking: Early in my career I worked on securing routing protocols for mobile ad hoc networks (ACM WiSe 2002, 900+ citations) and the challenge of establishing ad hoc security associations between devices that have no prior context (Computer Communications, 23:17, pp 1627-1637, 550+ citations). The latter work paved the way for subsequent work on Secure First Connect discussed above.

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 (Paper 5) and communication security (Paper 1) architectures, 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 [3]) to investigating the extent of mobile malware infection (Paper 4), which received wide press coverage, including by MIT Technology Review[4].

Mobile Trusted Computing: During the past decade, my colleagues and I have been pioneering academic research work on mobile trusted computing (Paper 3). Our early work on "On-board Credentials (ObC)" (Paper 8) has been deployed in Nokia smartphone platforms. The latest work in this direction is a system caleld Open-TEE which allows developers to easily make use of mobile trusted computing. Open-TEE (to appear in IEEE TrustCom 2015) was recently covered by The Register[5].

FULL LIST OF SUCCESSFUL TECHNOLOGY TRANSFERS

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 NSN 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*

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

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

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

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*

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

System Security and Privacy: for mobile and embedded devices, secure communications, platform security, usable security, data analytics for security/privacy, applied cryptography, secure electronic commerce.

Embedded and Distributed Systems: Operating systems, distributed algorithms, mobile computing infrastructures, Internet-of-Things, IP networks, ad-hoc networks.

CITATION RECORD

- Google Scholar Profile: `http://scholar.google.com/citations?user=0MqQ8AgAAAAJ` (**h-index: 40**)
- Academic Research Profile: `http://academic.research.microsoft.com/Author/267703`
- ACM Author Profile: `http://dl.acm.org/author_page.cfm?id=81100611941`
- ResearcherID Profile: `http://www.researcherid.com/rid/D-3182-2012` (**h-index: 10, #citations: 14.00/article**)

SUMMARY OF PUBLICATION RECORD

- **Refereed Publications**:
  - 12 Papers in peer-reviewed international journals and magazines
  - 1 Survey article in an international technology magazine
  - 75 Papers in international conferences or workshops
  - 6 Book chapters
- **Unrefereed Publications**:
  - 4 Invited papers in international conferences or workshops
  - 2 Books
  - 32 Technical reports

MOST IMPORTANT PUBLICATIONS

1. Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, Jean-Pierre Seifert: **Practical attacks against privacy and availability in 4G/LTE mobile communication systems**, (To appear in) Networks and Distributed Systems Conference (NDSS), February 2016.

2. Jian Liu, N. Asokan, Benny Pinkas: **Secure Deduplication of Encrypted Data without Additional Independent Servers**, Proceedings of ACM Conference on Computer and Communication Security (ACM CCS), Denver, October 2015. `http://doi.acm.org/10.1145/2810103.2813623` (Full version available as IACR ePrint report 2015/455, May 2015. `https://eprint.iacr.org/2015/455`)

3. 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`

4. 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`)

5. Pern Hui Chia, Yusuke Yamamoto, N. Asokan: **Is this app safe?: a large scale study on application permissions and risk signals**, In Proceedings of the 21st International World Wide Web Conference (WWW 2012), Lyon, France, April 2012. `http://dx.doi.org/10.1145/2187836.2187879`.

6. Nitesh Saxena, Jan-Erik Ekberg and Kari Kostiainen, N. Asokan : **Secure Device Pairing based on a Visual Channel** In IEEE Trans. Information Foresnsics and Security 6(1):28-38. 2011 `http://dx.doi.org/10.1109/TIFS.2010.2096217` (an earlier version appeared In Proceedings of the 2006 IEEE Symposium on Security and Privacy, pages 306–313, Berkeley/Oakland, May 2006. `http://doi.ieeecomputersociety.org/10.1109/SP.2006.35`)

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. `http://research.nokia.com/files/NRCTR2008007.pdf`)

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. System and method for establishing bearer-independent and secure connections (US 8,484,466)
2. Method and system for managing cryptographic keys (EP1561299, US 7,920,706)
3. System, method and computer program product for authenticating a data agreement between network entities (US 7,783,041)
4. Linked authentication protocols (US 7,707,412)
5. Authentication in a packet data network. (US 7,107,620, US 7,512,796, EP1273128)
6. Address acquisition. (US 6,959,009, US 7,920,575)

OTHER PATENTS

1. Implementation of an integrity-protected secure storage (US 9,171,187)
2. Method and apparatus to reset platform configuration register in mobile trusted module (US 9,087,198)
3. Methods and apparatus for reliable and privacy protecting identification of parties' mutual friends and common interests (US 9,003,486)
4. Method and apparatus for adjusting context-based factors for selecting a security policy (US 8,898,793)
5. Methods, apparatuses, and computer program products for bootstrapping device and user authentication (US 8,869,252)
6. Securing communication (US 8,769,284)
7. Credential provisioning (US 8,724,819)
8. Method, apparatus and computer program product for secure software installation (US 8,701,197)
9. Method and apparatus for selecting a security policy (US 8,621,656)
10. Method and apparatus to bind a key to a namespace (US 8,566,910)
11. Administration of wireless local area networks (US 8,532,304)
12. Requesting digital certificates (US 8,397,060)
13. Authenticated group key agreement in groups such as ad-hoc scenarios (US 8,386,782)
14. Methods, apparatuses, and computer program products for authentication of fragments using hash trees (US 8,352,737)
15. Secure data transfer (US 8,145,907)

16. Establishment of a trusted relationship between unknown communication parties (US 8,132,005)

17. Accessing protected data on network storage from multiple devices (US 8,059,818)

18. Method for remote message attestation in a communication system (US 7,913,086)

19. Information hiding non-interactive proofs-of-work (Korea 37764-KR-PCT)

20. Method for protecting electronic device, and electronic device (US 7,630,495)

21. System and method for dynamically enforcing digital rights management rules (US 7,529,929)

22. Secure backup and recovery using a key recovery service (Korea 808654)

23. Controlling delivery of certificates in a mobile communication system (US 7,526,642)

24. Method for sharing the authorization to use specific resources (US 7,343,014)

25. System and method of secure authentication and billing for goods and services using a cellular telecommunication and an authorization infrastructure (US 7,308,431)

26. Method, system, and devices for transferring accounting information (US 7,251,733)

27. Method, system and computer program product for secure ticketing in a communication device (US 7,207,060)

28. Method for applying electronic payment schemes in short-range e-commerce. (US 7,194,438)

29. IP mobility in a communication system (US 7,191,226)

30. 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)

31. Personal device, terminal, server and methods for establishing a trustworthy connection between a user and a terminal (US 7,149,895, EP 1026641)

32. System and method of bootstrapping a temporary public-key infrastructure from a cellular communication authentication and billing infrastructure. (US 7,107,248, EP1397787B1)

33. Addressing and routing in mobile ad hoc networks.

34. SIM based authentication mechanism for DHCPv4/v6 messages. (US 6,704,789, EP1175765B1)

EXTERNAL PRESENTATIONS

1. *The Quest for Usable Security* (**Invited talk**), University of Surrey workshop on Mobile Security December 2015
2. *Technology Transfer from Security Research Projects: A Personal Perspective* (**Invited keynote**), at 20th Nordic IT Security Conference (NordSec), KTH, Stockholm, Sweden. October 2015
3. *The Quest for Usable Security* (**Invited talk**), Android Security Symposium, Vienna, Austria (video: `https://youtu.be/gVPkFV5Zg2c`) September 2015
4. *How Far Removed Are You? Scalable Privacy-Preserving Estimation of Social Path Length* (Invited talk) University of Oxford, Oxford, United Kingdom March 2015
5. *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
6. *On Mobile Malware* (Invited talk), School of Computer Science Colloquium, McGill University, Montréal, Canada. December 2014
7. *Technology Transfer from Security Research Projects: A Personal Perspective* (**Invited lecture**), at Cybersecurity and Privacy (CySeP) Winter School, KTH, Stockholm, Sweden. October 2014
8. *On Mobile Malware* (**Invited talk**), ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Oxford, United Kingdom. July 2014
9. *On Mobile Malware* (Invited talk), NEC Labs Europe, Heidelberg, Germany. January 2014
10. *On Mobile Malware* (Invited talk), CrySP Speaker Series, University of Waterloo, Canada. (video: `https://crysp.uwaterloo.ca/events/20131216-Asokan.mp4`) December 2013
11. *The Untapped Potential of TEEs on Mobile Devices* (**Invited keynote** speech), Financial Cryptography and Data Security Conference (FC), Okinawa, Japan. April 2012
12. *Mobile Platform Security Architectures* (**Invited keynote** speech), 11th Smart Card Research and Advanced Application Conference (CARDIS), Graz, Austria. November 2012
13. *Context Profiling for Mobile Devices* (Invited talk), Securing Clouds & Mobility Track, Intel European Research & Innovation Conference (ERIC 12), Barcelona, Spain. October 2012
14. *The Case for Usable Mobile Security* (Invited talk), Department of Computer Science, University of Helsinki. August 2012
15. *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
16. *The Case for Usable Mobile Security* (**Invited Keynote** speech), Jaffna University International Research Conference (JUICE-2012), University of Jaffna, Sri Lanka. July 2012
17. *Solutions for Mobile Security and Privacy Protection* (**Invited Keynote** speech), Trust in Digital Life workshop, Biel, Switzerland. March 2012

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

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

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

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

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

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

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

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

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

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

28. *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

29. *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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sat, Feb 13, 2016