RFIDsec14

The 10th Workshop on RFID Security

WiSec 2014

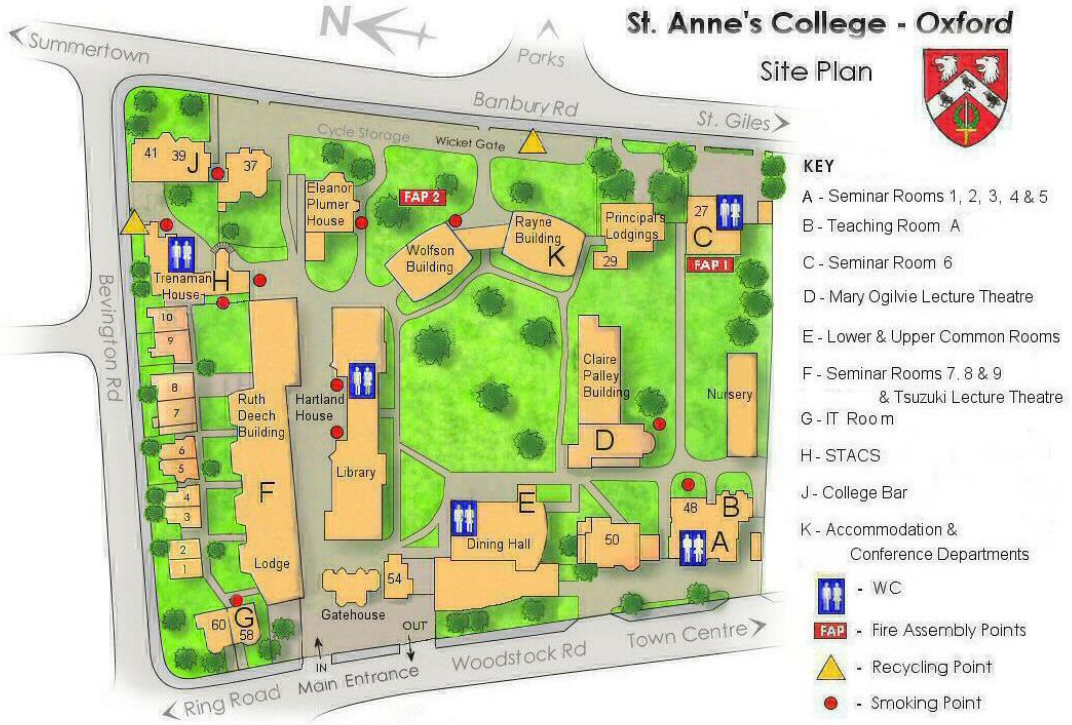
7th ACM Conference on Security and Privacy in Wireless and Mobile Networks

21st –25th July 2014
St. Anne's College, Oxford

Venues

Most of the scheduled events take place in St Anne's College:

- Tutorials in **Seminar Room 8 (F)**
- RFIDSec sessions on Tuesday in the **Tsuzuki Lecture Theatre (F)**
- All other technical programme sessions in **Mary Ogilvie Lecture Theatre (D)**
- Breakfast (for those in College Accommodation) in the **Dining Hall**
- Monday and Tuesday lunches in the **Ruth Deech building (F)**
- Wednesday – Friday lunches in the **Marquee**
- Demo/Poster Session (Wednesday) **Marquee**



The **RFIDSec Reception** on Monday evening is at **Department of Computer Science. (Enter from Keble Road).** The shortest walking route is via the *Wicket Gate* on Banbury Road. The code for access via the gate is ******.

The WiSec/RFIDSec **Banquet** on Wednesday is at **The Queen's College** (High Street). Allow 10-15 minutes to walk there from St. Anne's College.

Oxford Map – other venues

RFIDSec'14 Invited Talk (Tuesday 9:15am – 10:00am)

Clustering Distance Bounding Protocols

Prof. Gildas Avoine, INSA Rennes

Abstract: Distance bounding protocols are security countermeasures designed to thwart relay attacks. Such attacks consist in relaying messages exchanged between two parties, making them believe they communicate directly with each other. Although distance bounding protocols have existed since the early nineties, this research topic resurrected with the deployment of contactless systems, against which relay attacks are particularly impactful. Given the impressive number of distance bounding protocols that are designed every year, it becomes urgent to provide researchers and engineers with a methodology to fairly compare the protocols in spite of their various properties. After reviewing the literature of distance bounding protocols, we will introduce in this talk a methodology based on concepts from the decision making field in order to compare distance bounding protocols.

Bio: Gildas Avoine is a professor of Information Security and Cryptography at INSA Rennes in France and UCL in Belgium, and a member of the Institut Universitaire de France. Previously, he was a researcher at the MIT (USA) in the CSAIL, and at the EPFL (Switzerland) in the LASEC, where he obtained a PhD degree in cryptography. He did his undergrade studies at the University of Caen (France) where he received a Bachelor degree in mathematics and Bachelor and Master degrees in computer science. Gildas Avoine's main research area is information security, which he addressed with a cryptographic approach. His topics of interest include privacy models, lightweight authentication, distance bounding protocols, cryptanalytic time-memory trade-offs, and forensics. His current research focuses on security and privacy in ubiquitous computing systems, in particular radio-frequency identification.

ACM WiSec 2014 Invited Talk (Thursday, 9:00am – 10:00am)

On Mobile Malware Infections

Prof. N. Asokan, Aalto University

Abstract: Concerns about mobile malware are not new. There is a steady stream of news stories about the exponential growth of malware targeted at specific smartphone operating systems. Yet, anecdotal evidence seems to suggest that malware infection of smartphones in the wild is not at the same scale as malware infection of personal computers. Recently, we set out to accurately measure malware infection rates on Android devices. (se-sy.org/projects/malware/) In this talk, I will describe our experiences, some lessons learnt, and our attempts at using inexpensive risk indicators to predict susceptibility of a device for infection.

Bio: N. Asokan is a professor of computer science at University of Helsinki and professor of computer science and engineering at Aalto University. Prior to joining academia, he spent over fifteen years in industrial research at IBM Zurich Research Laboratory and Nokia Research Center. Asokan serves on the steering group of ACM WiSec. For more information about his work, see asokan.org/asokan

Talks

Keynote Speaker (Wednesday, 9:15am – 10:00am)

IoT — Connecting the Unconnected Securely
John O'Donnell, Cisco

Synopsis: In the last 12 months, the Internet of Things (IoT) has gained tremendous market momentum with strategic investments from all of the major IT companies and governments around the world. IoT promises massive gains in efficiency, business growth and quality of life. In the next 7 years, 27 billion new devices will connect to the Internet, with half of all data traffic being generated by IoT.

Cisco's go to market in this area is the Internet of Everything (IoE), which combines the things, with processes, data and people to create a holistic approach to derive value from the proliferation of these connected devices. In this new world we will need new infrastructure that's much more scalable, secure, and intelligent than ever before to "connect the unconnected". Big data generated by things will deliver new insights and predictions. This next wave of the Internet will touch every aspect of our lives: manufacturing, transportation, smart cities, energy, agriculture and health care which will all be transformed. Ultimately IoE is about the ability to get the right information to the right person at the right time and doing it in volume. For both private and public sectors.

John O'Donnell, Cisco's IoE pre sales consultants manager for EMEAR and APJC, will explore these topics, discuss some of the challenges and the important roles that wireless and security has to play in realising the opportunities.

Bio: John O'Donnell is Cisco's Internet of Everything (IoE) Pre Sales Consultants Manager across EMEAR & APJC. Together with his team of consultants, his key objective is to work with Cisco's Customers and Partners to articulate and demonstrate how IoE architectures and solutions can be applied to drive business transformation across all walks of industry and government.

John has a passion for IoE, and the positive impact it can have on society and the value it can and will bring to corporations, strongly believing we are just at the dawn of the IoE era, and the immense value it will enable.

John has a strong history of driving innovative technologies enabling customers to embrace different ways of conducting business and optimizing business operations. Up until August 2013 he led the pre sales consultants team for Cisco's Connected Safety & Security Solutions on a global basis. In the late 1990's and early 2000's John was instrumental in driving adoption of Cisco Unified Communications within Public Sector and other sectors in the UK, advising customers how to migrate from their proprietary silo based PBX environments to open IP based environments.

John holds an Electronics and Electrical Engineering from Loughborough University in the UK and has worked for Cisco 16 years. He lives with his family in Buckinghamshire and enjoys sports, outdoor activities and travelling.

Seminar Room 8

Tutorial 1 (9:30am – 12:30pm)

Side-Channel Attacks 101: Theory and Practice

David Oswald/Timo Kaspe/Falk Schellenberg, Ruhr-Universität Bochum

Description:

Implementation attacks and side-channel analysis are techniques to break analytically secure ciphers. Instead of focusing on the mathematical properties, side-channel attacks target the physical implementation of cryptography, e.g., on a microcontroller or an FPGA.

This tutorial starts with an in-depth introduction into the topic, covering methods like timing attacks and simple/differential power analysis (SPA/DPA). With these techniques, unprotected implementations of standard ciphers like RSA, ECC, or AES can often be broken within minutes. Besides, the tutorial also presents typical measurement setups for the acquisition of side-channel signals and other implementation attacks, for instance fault injection.

The second part of the tutorial deals with the practical application of side-channel analysis, focusing on several real-world case studies. In particular, for RFID systems, our 2011 side-channel attacks on the DESFire MF3ICD40 smartcard are presented.

Based on the case studies, the impact of attacks on real systems is evaluated and compared. Finally, possible countermeasures on different levels (hardware, software, backend) are discussed.

Lunch (1:00pm – 2:00pm)

Tutorial 2 (2:00pm – 5:00pm)

Trusted Execution Environments on Mobile Devices

Kari Kostiainen, ETH Zurich

Description:

A trusted execution environment (TEE) is a secure processing environment that is isolated from the “normal” processing environment where the device operating system and applications run. The first mobile phones with hardware-based TEEs appeared almost a decade ago, and today almost every smartphone and tablet contains a TEE like ARM TrustZone. Despite such a large-scale deployment, the use of TEE functionality has been limited for developers. With emerging standardization this situation is about to change. In this tutorial, we explain the security features provided by mobile TEEs and describe On-board Credentials (ObC) system that enables third-party TEE development. We discuss ongoing TEE standardization activities, including the recent Global Platform standards and the Trusted Platform Module (TPM) 2.0 specification, and identify open problems for the near future of mobile hardware security.

RFIDSec Reception (6:00pm – 7:30pm)

Department of Computer Science

Tsuzuki Lecture Theatre

Welcome (9:00am – 9:15am)

RFIDSec'14 Invited Talk (9:15am – 10:00am)

- *Prof. Gildas Avoine, INSA Rennes*
  Clustering Distance Bounding Protocols

Coffee (10:00am – 10:30am)

Session 1: Power Efficiency (10:30am – 12:00noon)

- *Peter Pessl and Michael Hutter.* Curved Tags – A Low-Resource ECDSA Implementation tailored for RFID Tags
- *Krishna Pabbuleti, Deepak Mane and Patrick Schaumont.* Energy Budget Analysis for Signature Protocols on a Self-powered Wireless Sensor Node (short)
- *Michael Weiner, Salvador Manich and Georg Sigl.* A Low Area Probing Detector for Power Efficient RFID Security ICs

Lunch (12:00noon – 2:00pm)

Session 2: Privacy (2:00pm – 3:30pm)

- Lejla Batina, Jens Hermans, Jaap-Henk Hoepman and Anna Krasnova. High-speed dating — Privacy-preserving attribute matching for RFID
- *Rui Figueiredo, André Zúquete and Tomás Oliveira E Silva.* Massively parallel identification of privacy-preserving vehicle RFID tags
- *Nan Li, Yi Mu, Willy Susilo, Fuchun Guo and Vijay Varadharajan.* Privacy-preserving Authorized RFID Authentication Protocols (short)

Coffee (3:30pm – 4:00pm)

Session 3: Authentication and Side Channels (4:00pm – 5:30pm)

- *Luigi Sportiello.* ePassport: Side Channel in the Basic Access Control
- *Frederik Armknecht, Matthias Hamann and Vasily Mikhalev.* Lightweight Authentication Protocols on Ultra-Lightweight RFIDs — Myths and Facts
- Xin Ye, Cong Chen and Thomas Eisenbarth. Non-Linear Collision Analysis

ACM WiSec 2014 and RFIDSec 2014

Mary Ogilvie Lecture Theatre

Welcome (9:00am – 9:15am)

Keynote (9:15am – 10:00am)

- *John O'Donnell, Cisco*
  IoT — Connecting the Unconnected Securely

Coffee (10:00am – 10:30am)

WiSec Session 1: Smart Phone 1 (10:30am – 12:00noon)

- *David Barrera, Daniel McCarney, Jeremy Clark and Paul C. van Oorschot.* Baton: Certificate Agility for Android's Decentralized Signing Infrastructure
- *Adwait Nadkarni, Vasant Tendulkar and William Enck.* NativeWrap: Ad Hoc Smartphone Application Creation for End Users
- *Fangfang Zhang, Heqing Huang, Sencun Zhu, Dinghao Wu and Peng Liu.* ViewDroid: Towards Obfuscation-Resilient Mobile Application Repackaging Detection

Lunch (12:00noon – 2:00pm)

Poster/Demo Session (1:15pm – 2:30pm)

RFIDSec Session 4: Ciphers, Key Exchange, and Implementations (2:30pm – 4:00pm)

- *Chitra Javali, Girish Revadigar, Lavy Libman and Sanjay Jha.* SeAK: Secure Authentication and Key Generation Protocol based on Dual Antennas for Wireless Body Area Networks (short)
- *Hannes Gross, Michael Hutter, Erich Wenger and Honorio Martin Gonzalez.* PIONEER — a Prototype for the Internet of Things based on an Extendable EPC Gen2 RFID Tag
- *Kostas Papagiannopoulos.* High throughput in slices: the case of PRESENT, PRINCE and KATAN64 ciphers
- Abhishek Kumar, Somitra Kumar Sanadhya, Praveen Gauravaram, Nasour Bagheri, Javad Alizadeh, Mohammad Reza Aref, Hoda A. Alkhzaimi and Martin M. Lauridsen. Cryptanalysis of SIMON Variants with Connections (short)

Coffee (4:00pm – 4:30pm)

/continues

WiSec Session 2: Sensing and Embedded Systems (4:30pm – 6:10pm)

- *Stylianos Gisdakis, Thanassis Gianetsos and Panos Papadimitratos.* SPPEAR: Security & Privacy-Preserving Architecture for Mobile Crowd-Sensing Applications
- *Jun Han, Yue-Hsun Lin, Adrian Perrig and Fan Bai.* MVSec: Secure and Easy-to-Use Pairing of Mobile Devices with Vehicles (short)
- *Andrei Costin and Aurélien Francillon.* A dangerous "pyrotechnic composition": fireworks, embedded wireless and insecurity-by-design (short)
- *Ira Ray Jenkins, Rebecca Shapiro, Sergey Bratus, Ryan Speers, Travis Goodspeed and David Dowd.* Speaking the Local Dialect: Exploiting differences between IEEE 802.15.4 Receivers with Commodity Radios for fingerprinting, targeted attacks, and WIDS evasion (short)

Banquet (7:00pm drinks; meal at 7:30pm)

The Queen's College (15 minutes' walk from St Anne's College; see p3)

Thursday 24th July: ACM WiSec 2014

Mary Ogilvie Lecture Theatre

WiSec Invited Talk (9:00am – 10:00am)

- *Prof. N. Asokan, Aalto University*
  On Mobile Malware Infections

Coffee (10:00am – 10:30am)

Session 3: Location Privacy

- *Arijit Banerjee, Dustin Maas, Maurizio Bocca, Neal Patwari and Sneha Kasera.* Violating Location Privacy Through Walls by Passive Monitoring of Radio Windows
- *Luke Hutton, Tristan Henderson and Apu Kapadia.* "Here I am, now pay me!'': privacy concerns in incentivised location-sharing systems (short)
- *Alfredo Rial, Michael Herrmann, Claudia Diaz and Bart Preneel.* Privacy-Preserving Location-Sharing-Based Services
- *Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Capkun and David Basin.*Detection of GPS Spoofing Attacks in Power Grids (short)

Lunch (12:15pm – 2:00pm)

Session 4: Jamming and Anti-Jamming (2:00pm – 3:30pm)

- *Daniel S. Berger, Francesco Gringoli, Nicolò Facchi, Ivan Martinovic and Jens Schmitt.*Gaining Insight on Friendly Jamming in a Real-World IEEE 802.11 Network
- *Bruce Debruhl, Christian Kroer, Anupam Datta, Tuomas Sandholm and Patrick Tague.*Power Napping with Loud Neighbors: Optimal Energy-Constrained Jamming and Anti-Jamming
- *Hanif Rahbari and Marwan Krunz.* Friendly CryptoJam: A Mechanism for Securing Physical-Layer Attributes

Coffee (3:30pm – 4:00pm)

Session 5: Smart Phone 2 (4:00pm – 5:30pm)

- *Wenhui Hu, Damien Octeau, Patrick McDaniel and Peng Liu.* Duet: Library Integrity Verification for Android Applications
- *Zhen Xie and Sencun Zhu.* GroupTie: Toward Hidden Collusion Group Discovery in App Stores
- *Mengtao Sun and Gang Tan.* NativeGuard: Protecting Android Applications from Third-Party Native Libraries

Barbeque (7:00pm – 9:00pm)

St. Anne's College: Marquee

Mary Ogilvie Lecture Theatre

Session 6: Wireless and PHY (9:00am – 10:20am)

- *Nicholas Kolokotronis, Alexandros Katsiotis and Nicholas Kalouptsidis.* Attacking and Defending Lightweight PHY Security Schemes for Wireless Communications (short)
- *Ibrahim Ethem Bagci, Utz Roedig, Matthias Schulz and Matthias Hollick.* Gathering Tamper-Evidence in Wi-Fi Networks Based on Channel State Information (short)
- *Pieter Robyns, Bram Bonné, Peter Quax and Wim Lamotte.* Exploiting WPA2-Enterprise Vendor Implementation Weaknesses through Challenge Response Oracles (short)
- *Frederik Möllers, Sebastian Seitz, Andreas Hellmann and Christoph Sorge.* Extrapolation and Prediction of User Behaviour from Wireless Home Automation Communication (short)

Coffee (10:20am – 11:00am)

Session 7: Smart Phone 3 (11:00am – 12:40pm)

- *Sashank Narain, Amirali Sanatinia and Guevara Noubir.* Single-stroke Language-Agnostic Keylogging using Stereo-Microphones and Domain Specific Machine Learning
- *Jiaqi Tan, Utsav Drolia, Rolando Martins, Rajeev Gandhi and Priya Narasimhan.* CHIPS: Content-based Heuristics for Improving Photo Privacy for Smartphones (short)
- *Alessandro Armando, Gabriele Costa, Alessio Merlo and Luca Verderame.* Enabling BYOD through Secure Meta-Market
- *Jagdish Prasad Achara, Mathieu Cunche, Vincent Roca and Aurelien Francillon.* WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission (short)

Lunch (12:40pm – 2:00pm)

- *Glenn Wilkinson.* DEMO: Practical Tracking, Profiling, and Data Interception
- *Jiaqi Tan, Utsav Drolia, Rajeev Gandhi and Priya Narasimhan.* POSTER: Towards Secure Execution of Untrusted Code for Mobile Edge-Clouds
- *Martin Strohmeier and Ivan Martinovic.* POSTER: Detecting False-Data Injection Attacks on Air Traffic Control Protocols
- *Panagiotis Andriotis, Theo Tryfonas and Zhaoqian Yu.* POSTER: Breaking the Android Pattern Lock Screen with Neural Networks and Smudge Attacks
- *Tristan Henderson and David Kotz.* POSTER: CRAWDAD: A Wireless Network Data Archive for WiSec Researchers
- *Matthias Schäfer, Vincent Lenders and Jens Schmitt.* POSTER: Secure Path Verification using Mobility-Differentiated ToA
- *Gregory Nazario, Michael Rosen, Lawrence Jackson, Michael Hankowsky, Bruce Debruhl and Patrick Tague.* POSTER: Modeling Cross-Layer Mischief in Wireless Networked Control Systems
- *Yuchen Zhao, Juan Ye and Tristan Henderson.* POSTER: Recommending Location Privacy Preferences in Ubiquitous Computing
- *Jan Henrik Ziegeldorf, Nicolai Viol, Martin Henze and Klaus Wehrle.* POSTER: Privacy-preserving Indoor Localization
- *Andrei Costin and Jonas Zaddach.* POSTER: Firmware.RE: Firmware Unpacking and Analysis as a Service
- *Andrew Paverd.* POSTER: Enhancing Privacy in Location-Based Services using Trustworthy Remote Entities
- *Amirali Sanatinia, Sashank Narain and Guevara Noubir.* POSTER: WiFi AP Infection Spread
- *Nicholas Micallef, Gunes Kayacik, Mike Just, Lynne Baillie and David Aspinall.* POSTER: Sensor-Based Authentication: Usable? Secure? Efficient?

Committees: ACM WiSec 2014

Programme Committee
Claude Castelluccia, INRIA, France (chair)
Patrick Traynor, University of Florida, USA (chair)
David Barrera, Carleton University, Canada
Erik-Oliver Blass, Northeastern University, USA
Elie Bursztein, Google, USA
Kevin Butler, University of Oregon, USA
Srdjan Capkun, ETH Zürich, Switzerland
Nicolas Christin, Carnegie Mellon University, USA
Emiliano De Cristofaro, University College London, UK
Adrienne Felt, Google, USA
Aurélien Francillon, Eurecom, France
Julien Freudiger, PARC, USA
Thorsten Holz, Ruhr-Universität Bochum, Germany
Murtuza Jadliwala, Wichita State University, USA
Sanjay Jha, University of New South Wales, Australia
Apu Kapadia, Indiana University, USA
Frank Kargl, University of Ulm, Germany
Yongdae Kim, KAIST, Republic of Korea
Engin Kirda, Northeastern University, USA
Cedric Lauradoux, INRIA, France
Loukas Lazos, University of Arizona, USA
Vincent Lenders, Armasuisse, Switzerland
David Lie, University of Toronto, Canada
Long Lu, Stony Brook University, USA
Di Ma, University of Michigan-Dearborn, USA
Luigi Mancini, Università di Roma La Sapienza, Italy
Rene Mayrhofer, Upper Austria University of Applied Sciences, Austria
Refik Molva, EURECOM, France
Guevara Noubir, Northeastern University, USA
Panos Papadimitratos, KTH, Sweden
Bryan Parno, Microsoft Research, USA
Roberto Di Pietro, Università di Roma Tre, Italy
Christina Pöpper, Ruhr-University Bochum, Germany
Axel Poschmann, PACE/Nanyang Technological University, Singapore
Kasper Bonne Rasmussen, University of Oxford, UK
Ahmad-Reza Sadeghi, Technische Universität Darmstadt, Germany
Jens Schmitt, TU Kaiserslautern, Germany
Micah Sherr, Georgetown University, USA
Reza Shokri, ETH Zürich, Switzerland
Claudio Soriente, ETH Zürich, Switzerland
Patrick Tague, Carnegie Mellon University, USA
Dirk Westhoff, Hochschule Furtwangen, Germany
Sencun Zhu, Penn State University, USA

General Chairs:
Andrew Martin, Department of Computer Science, University of Oxford, UK
Ivan Martinovic, Department of Computer Science, University of Oxford, UK

Programme Chairs:
Claude Castelluccia, INRIA, France
Patrick Traynor, University of Florida, USA

Publicity Chairs:
Kasper Rasmussen, University of California, Irvine, USA
Mathieu Cunche, INRIA, France
Publication Chair: Gergely Acs, INRIA, France
Poster/Demo Chair: Aurélien Francillon, Eurecom, France
Web Chair: Justin King-Lacroix, Department of Computer Science, University of Oxford, UK

Local Organisers:
Elizabeth Walsh, Department of Computer Science, University of Oxford, UK
Andrea Pilot, Department of Computer Science, University of Oxford, UK

Steering Committee
Gene Tsudik, University of California, Irvine, USA (chair)
N. Asokan, Aalto University and University of Helsinki, Finland
Srdjan Capkun, ETH Zurich, Switzerland
Claude Castelluccia, INRIA, France
Douglas Maughan, Department of Homeland Security, USA
Ahmad-Reza Sadeghi, Technische Universitat Darmstadt, Germany

Committees: RFIDSec 2014

Program Committee

Nitesh Saxena, University of Alabama at Birmingham, USA (Co-Chair)
Ahmad-Reza Sadeghi, Technische Universitat Darmstadt, Germany (Co-Chair)
Gildas Avoine, Université catholique de Louvain, Belgium
Lejla Batina, Radboud University Nijmegen, Netherlands
Srdjan Capkun, ETH Zürich, Switzerland
Mauro Conti, University of Padua, Italy
Bruno Crispo, University of Trento, Italy
Thomas Eisenbarth, Worcester Polytechnic Institute, USA
Aurelien Francillon, Institut Eurécom, France
Tzipora Halevi, Polytechnic Institute of New York University, USA
Gerhard Hancke, City University of Hong Kong, Hong Kong
Jaap-Henk Hoepman, Radboud University Nijmegen, Netherlands
Mehran Mozaffari Kermani, Rochester Institute of Technology, USA
Karl Koscher, University of Washington, USA
Kari Kostiainen, ETH Zürich, Switzerland
Farinaz Koushanfar, Rice university, USA
Yingjiu Li, Singapore Management University, Singapore
Mark Manulis, University of Surrey, United Kingdom
Roberto Pietro, Roma Tre University of Rome, Italy
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Pankaj Rohatgi, Cryptography Research Inc., USA
Joshua Smith, University of Washington, USA
Ersin Uzun, PARC, USA
Jonathan Voris, Columbia University, USA
Avishai Wool, Tel Aviv University, Israel

General Chairs

Andrew Martin, University of Oxford, UK
Ivan Martinovic, University of Oxford, UK

Program Chairs

Nitesh Saxena, University of Alabama at Birmingham, USA
Ahmad-Reza Sadeghi, Technische Universitat Darmstadt, Germany

Publicity Chair

Jonathan Voris, Columbia University, USA

Web Chairs

Mihai Bucicoiu, Technische Universitat Darmstadt, Germany
Babins Shrestha, University of Alabama at Birmingham, USA

Steering Committee

Gildas Avoine, UCL, Louvain-la-Neuve, Belgium (chair)
Lejla Batina, RU Nijmegen, The Netherlands; KULeuven, Belgium
Srdjan Capkun, ETHZ, Switzerland
Michael Hutter, TU Graz, Austria
Yingjiu Li, Singapore Management University, Singapore
Christof Paar, RUB, Germany
Bart Preneel, KULeuven, Belgium
Patrick Schaumont, Virginia Tech, USA
Jörn-Marc Schmidt, TU Graz, Austria

Programme at a Glance

Registration desk open daily from 8.30am. Morning sessions start at 9:00am.
Break and lunch times vary: see full programme (inside) for details.

Tutorials | RFIDSec | ACM WiSec | RFIDSec and ACM WiSec

	Morning	Afternoon	Evening
Monday 21st July	**Tutorial 1:** Side-Channel Attacks 101	**Tutorial 2:** Trusted Execution Environments on Mobile Devices	**Welcome Reception** (Dept. of Computer Science)
Tuesday 22nd July	**Invited Talk**: Clustering Distance Bounding Protocols Prof. Gildas Avoine	**Session 2:** Privacy	
	Session 1: Power Efficiency	**Session 3:** Authentication and Side Channels	
Wednesday 23rd July	**Keynote***: IoT Security,* John O'Donnell, Cisco	**Poster/Demo Session**	**Banquet** (The Queen's College)
		Session 4: Ciphers, Key Exchange, and Implementations	
	Session 1: Smartphone 1	**Session 2:** Sensing and Embedding	
Thursday 24th July	**Invited Talk:** *On Mobile Malware Infections*, Prof. N. Asokan	**Session 4:** Jamming and Anti-Jamming	**BBQ** (St Anne's College)
	Session 3: Location Privacy	**Session 5:** Smartphone 2	
Friday 25th July	**Session 6:** Wireless and PHY		
	Session 7: Smartphone 3		

On **Wednesday 23rd July**, RFIDSec attendees are welcome to attend the WiSec sessions, and *vice versa.*

Internet Access: At registration, you will receive personalized credentials for WiFi access, together with a statement of the University's rules regarding this service. This access will work in most University buildings, as will the ***eduroam*** service.