Smart Cards, Tokens, Security and Applications

Keith Mayes · Konstantinos Markantonakis
Editors

Smart Cards, Tokens, Security and Applications

Second Edition

Springer

Editors
Keith Mayes
Director of the Information Security Group,
Head of the School of Mathematics and
Information Security
Royal Holloway, University of London
Egham, Surrey
UK

Konstantinos Markantonakis
Smart Card Centre, Information Security
Group
Royal Holloway, University of London
Egham, Surrey
UK

ISBN 978-3-319-50498-8 ISBN 978-3-319-50500-8 (eBook)
DOI 10.1007/978-3-319-50500-8

Library of Congress Control Number: 2016959517

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

I would like to dedicate this book to Susan, George and Amelia, to my mother and to the memory of my late father

Keith Mayes

I would like to dedicate this book to Maria, Eleni and Georgios

Konstantinos Markantonakis

Founders Message

The ISG Smart Card Centre (SCC) was established in 2002 as a centre of excellence to complement the world leading work of the Information Security Group (ISG), which was established in 1990. With the ISG having pioneered information/cybersecurity for more than a quarter of a century, the SCC still feels quite new, but at 14+ years old it is clearly something of enduring substance. This is testament to the vision and commitment of the SCC Founders, who saw the need for a UK-based centre involved in academic research, training and expert advisory activities, in the areas of smart cards, RFIDs and embedded systems security. Of course technology is always changing, and today, the SCC is also interested in the security of Near-Field Communication (NFC) mobile phones/devices, vehicular/transport security and the enormous challenges of safeguarding the Internet of Things (IoT), and critical infrastructure in general. However, the need to consider implementation security and attack resistance, as well as secure design, is more vital than ever. This is a principle that we have instilled in the many M.Sc. students who have studied and completed projects in the SCC, with the aid of the course text book. The book was originally published in 2008 and came about because no other text could offer the breadth and depth of content needed for the M.Sc. Today, the book is a reference found on many bookshelves (physical or virtual!) beyond academia and this new edition aims to keep the content fresh, relevant and useful.

The Founders continue to be proud of their association with this book and of their pioneering efforts that brought about the SCC.

The Founders:

Professor Michael Walker OBE
Founder Director of Vodafone Group Research and Development
Professor of Telecommunications (Vodafone Chair)
Royal Holloway, University of London

Dr. Klaus Vedder
Group Senior Vice President
Giesecke & Devrient GmbH

Professor Fred Piper
Founder Director of the Information Security Group
Royal Holloway, University of London

Professor Keith Mayes
Founder Director of the ISG Smart Card Centre
Director of the Information Security Group
Head of the School of Mathematics and Information Security
Royal Holloway, University of London

Foreword

The idea of inserting a chip into a plastic card is nearly as old as public-key cryptography. The first patents are now 40 years old, but practical, massive application deployment started only twenty years ago due to limitations in storage and processing capacities of past circuit technology. Today, new silicon geometries and cryptographic processing refinements lead the industry to new generations of cards and more ambitious applications.

Over the last two decades, there has been an increasing demand for smart cards from national administrations and large companies such as telephone operators, banks and insurance corporations. More recently, other identity and payment markets have opened up with the increasing popularity of home networking and Internet and the advent of International Civil Aviation Organization (ICAO) passport standards.

At the same time, cryptographic hardware engineering grew into an active research field with flagship conferences and journals such as the Conference on Cryptographic Hardware and Embedded Systems (CHES) and the Journal of Cryptographic Engineering. Over a hundred Ph.D. theses on side-channel attacks are defended each year throughout the world and attack contests regularly benchmark the community's level of knowledge.

The traditional carrier for a conventional smart card is a plastic rectangle on which can be printed information concerning the application or the Issuer (even advertising) as well as readable information about the cardholder (as for instance, a validity date or a photograph). This carrier can also include a magnetic stripe or a bar code label. An array of eight contacts is located on the micromodule in accordance with the ISO 7816 standard, but only six of these contacts are normally connected to the chip, which is (usually) not visible. The contacts are assigned to power supplies, ground, clock, reset and a serial data communication link (commonly called I/O). However, over the last years, mainstream protocols and technologies such as USB, http and Simple Object Access Protocol (SOAP) were adopted by the card industry and the cards form factor has evolved. In the same time, contactless cards have become increasingly popular. New Trusted Execution

Environments have recently matured and start to be deployed in smartphones. These can be regarded as non-detachable smart cards that, in essence, are subject to the same design and security constraints as those of usual smart cards.

Current smart card CPUs range from simple 8-bit microcontrollers to sophisticated 32-bit architectures. RAM capacities, historically limited to a few hundreds of bytes, are steadily increasing. ROM and Electrically Erasable Programmable Read-Only Memory (EEPROM) are being progressively replaced by Flash, whilst native execution is commonly substituted by Java applets.

Cutting one's way through such a technology-rich environment requires several years of industrial experience or a very thorough reference, such as this book.

Throughout the years of research in Royal Holloway's Smart Card Centre, Kostas and Keith have invented, implemented and benchmarked an incredible number of card technologies. Their industrial background and academic approach are, to my knowledge, unique in the field. The number of their alumni is impressive.

I hope that you will enjoy reading and learning from this book as much as I did.

August 2016

Prof. David Naccache
Laboratoire d'informatique de l'Ecole normale supérieure
Université Paris II, Panthéon-Assas

Preface

When the first edition of this book was published back in 2008, the scope was anything to do with smart cards and security tokens in the widest sense. The aim was in fact to provide a complete story, looking at a cross section of technologies, processes, applications and real-world usage. The original motivation for the book was to provide a suitable reference text for the Masters course in Information Security, run by the Information Security Group (ISG) at Royal Holloway, University of London (RHUL). However, as the planning for the book advanced we realised that various industries and government departments can become quite narrow in their understanding of smart cards/RFIDs and that looking across industry and across roles (such as technical, business and logistics) could be beneficial for a much wide range of readers. Eight years on, in this second edition, we find we have new material to cover, whilst surprisingly, very little of the old material is redundant. Although smart cards and RFIDs are still at the core of what we do, increasingly we are involved in general embedded systems, mobile device security, trusted execution and the all-encompassing Internet of Things (IoT). Indeed, the course for which the book was written is now called "Smart Cards, RFIDs and Embedded Systems Security" and our Smart Card Centre is now the "Smart Card and IoT Security Centre"!

One constant across the years is that to deliver such breadth of information requires input from many experts and so we are very pleased and proud of the calibre of the authors and reviewers that have made this book possible. We hope that you will enjoy this book and find it a useful guide and reference.

Structure of the Book

This book consists of eighteen chapters. Each chapter is a completely autonomous contribution in a chained discussion which aims to bring researchers, practitioners and students up to speed with the recent developments within the smart card arena. In order to enhance the reader experience, each book chapter contains its own

abstract, introduction, main body and conclusion sections. Furthermore, bibliography resources can be found at the very end of each chapter. The following list provides a more detailed overview of the topics that are discussed in the different chapters of this book.

Chapter 1 provides an introduction to a very wide range of smart card-related issues. It surveys the different types of cards, tokens, and it also considers the main types and capabilities of popular applications utilising smart card technology. The chapter is considered as a good starting point for newcomers to the field and perhaps those that have perhaps focussed on one business or technical area.

Chapter 2 discusses the different steps in the smart card production chain. The analysis covers all the main steps during the smart card manufacturing phase starting with the production of the card body, chip moulding and smart card personalisation and delivery. Finally, it concludes with current and future trends and challenges.

Chapter 3 provides an overview of the most widely utilised smart card operating systems and platforms that enable multiple applications to be securely managed and reside in the same smart card.

Chapter 4 discusses the role of the Subscriber Identity Module (SIM) in the mobile telecommunications industry and describes the associated standards. It presents the authentication and ciphering processes in some depth and provides a practical comparison between the two technologies prior to exploring further value-added service and toolkit features. Finally, it provides some insight into the future evolution of technology.

Chapter 5 examines the role of smart card technology within the financial payments industry. It examines how the credit card industry has evolved over the decades and explains some of the issues with magnetic stripe card technology. Subsequently, it presents the main features of smart card technology in the light of the EMV card specifications. The discussion continues with 3D-secure and token authentication.

Chapter 6 deals with the issues around content protection in the satellite TV industry. In particular, it examines the commercial motivation as the driving force behind content protection, how smart card security is utilised in order to provide the necessary functionality and finally highlights how a typical pay-TV system operates.

Chapter 7 provides an overview of the Trusted Platform Module (TPM) and highlights commonalities and differences with smart cards. It provides an introduction to the security mechanisms provided by the TPM and provides a guide to the associated standards and literature.

Chapter 8 explains how Common Criteria evolved, how it is defined and how it is used in practice. More importantly, it examines how Common Criteria is applied to the complex and demanding field of smart card security evaluations.

Chapter 9 focuses on the various attacks and countermeasures that apply to smart cards. As many applications rely on cryptographic algorithms for sensitive operations, this chapter focuses on the attacks that could affect smart cards performing cryptographic operations. Furthermore, it provides references to the corresponding

countermeasures and emphasises the need for rigorous design, implementation and test of cryptographic algorithms and their underlying host platforms.

Chapter 10 provides a brief overview of the wide range of issues associated with the smart card application development processes. In particular, it examines the development of an application for the popular Java Card platform. It also highlights practical issues around application development and monitoring tools. Finally, it looks into development of the mobile phone applications that can exploit SIM and USIM card capabilities by using it as a trusted security element.

Chapter 11 analyses the use of the smart card within the telecommunications industry as a managed platform. It examines how the mobile phone operators are using the necessary tools and technology in order to remotely update and enhance, over-the-air, the functionality of SIM and USIM cards.

Chapter 12 provides a valuable introduction to the main standards used to manage and access smart card readers connected to personal computers. Their main functionality is analysed and attached code samples aim to provide a detailed overview, but also to enable the reader to reuse them in order to quickly develop sample host applications that will communicate with smart cards. Mobile phone Application Program Interface (API) that can access smart cards, SIM card and Secure Elements is also included in this chapter.

Chapter 13 provides an introduction to the Radio Frequency Identification (RFID) concepts and also summarises the aspects most relevant to contactless smart card systems. Several different systems along with the operating principles are described. The chapter also provides an overview of the main Radio Frequency (RF) interface and communication theory along with the various RF standards. The chapter concludes with an overview of Near-Field Communication (NFC).

Chapter 14 explains how national requirements for eID cards and e-passports can be realised by utilising physical, logical and hardware functionality. Furthermore, it highlights the importance and requirements of the relevant standards.

Chapter 15 first examines the historical use of technology in smart cards before highlighting the future trends. It looks into the different options and choices which can be made within a smart card scheme along with the issues which affect the design of the card and its applications. Finally, it discusses issues around consumer demand and the drivers that will define the smart card technology of the future.

Chapter 16 describes how security challenges arise from a rapidly growing population of smart and/or embedded digital devices that can leverage, monitor and control systems and components in the physical world—known as the Internet of Things (IoT). This chapter outlines the means for addressing these challenges and introduces a proposed overall decision-making framework for developing an IoT security strategy.

Chapter 17 discusses the concepts behind the MULTOS smart card operating system and introduces the development environment and tools. It provides several examples of code to assist in explanations. It also briefly outlines possible future uses for MULTOS outside of smart cards.

Chapter 18 explains how a Trusted Execution Environment (TEE) provides an execution platform on a mobile device, isolated from the rest of the operating system and other applications: the chapter explores what constitutes a TEE and their various security features. Standardisation efforts related to TEEs and example implementations of TEEs are also outlined. Host Card Emulation (HCE) provides an alternative to "traditional" Near-Field Communication (NFC) card emulation by allowing an application on the host CPU of a mobile device to emulate a card and communicate directly with an external reader. HCE introduces new security risks to the mobile ecosystem, and this chapter illustrates how these can be managed to an acceptable level.

In order to make reading of this more convenient, we also provide a subject index at the very end of the book.

June 2016

Keith Mayes
Konstantinos Markantonakis
Royal Holloway, University of London, Egham, UK

Acknowledgements

We offer our sincere thanks to all those that helped bring about the second edition of this book. There are too many to mention them all, but a few names must appear here. Firstly, we would like to thank Mike Walker, Klaus Vedder and Fred Piper, for their vision and steadfast support of the Smart Card Centre (SCC). We must certainly not forget the companies that have sponsored the SCC over the years and especially Vodafone, Giesecke & Devrient, Transport for London, the UK Cards Association, ITSO and Orange Labs UK; as without them, there would be no SCC and no book. A book also needs authors and reviewers, and ours all deserve medals for their excellent contributions and their tested patience. Last, but definitely not least, we must marvel at the herculean efforts of Sheila Cobourne and Danushka Jayasinghe in helping to bring this book to print.

Contents

Editors and Contributors

About the Editors

Prof. Keith Mayes, B.Sc., Ph.D. CEng FIET A. Inst. ISP is the Director of the Information Security Group (ISG), and Head of the School of Mathematics and Information Security at Royal Holloway, University of London, which has been pioneering information/cybersecurity research and education since 1990. He is an active researcher/author with 100+ publications in numerous conferences, books and journals. His current research interests are diverse, including mobile communications, Near-Field Communication (NFC), mobile platform security, smart cards, Radio Frequency IDs (RFIDS), the Internet of Things, transport ticketing/system security, embedded systems and e-commerce. Keith joined the ISG in 2002, originally as the founder Director of the ISG Smart Card Centre, following a career in industry working for Pye TVT, Honeywell Aerospace and Defence, Racal Research and Vodafone. Keith is a Chartered Engineer, a Fellow of the Institution of Engineering and Technology, a Founder Associate Member of the Institute of Information Security Professionals, a Member of the Licensing Executives Society and an experienced company director and consultant.

Prof. Konstantinos Markantonakis B.Sc., M.Sc., MBA, Ph.D. (London) received his B.Sc. in Computer Science from Lancaster University in 1995, his M.Sc. in Information Security in 1996, his Ph.D. in 2000 and his MBA in International Management in 2005 from Royal Holloway, University of London. He is currently a Professor of Information Security in the Information Security Group in Royal Holloway, University of London. He is also the Director of the Information Security Group Smart Card Centre (SCC). His main research interests include smart card security and applications, secure cryptographic protocol design, key management, embedded system security and trusted execution environments, mobile phone operating systems/platform security, NFC/RFID/HCE security, grouping proofs, electronic voting protocols. He has published more than 140 papers in international conferences and journals. Since completing his Ph.D., he has worked as an independent consultant in a number of information security and smart card related projects. He has worked as multiapplication smart card manager in VISA International EU and as a Senior Information Security Consultant for Steer Davies Gleave. He is a member of the IFIP Working Group 8.8 on Smart Cards. Since June 2014, he is the vice-chair of IFIP WG 11.2 Pervasive Systems Security. He continues to act as a consultant on a variety of topics including smart card security, key management, information security protocols, mobile devices, smart card migration program planning/project management for financial institutions, transport operators and technology integrators.

Contributors

Raja Naeem Akram is working as a postdoctoral Research Assistant at the Information Security Group (ISG), Royal Holloway, University of London, and is involved with the research projects involving digital avionics and payment systems. Previously, Raja worked as research fellow at the Cyber Security Lab, Department of Computer Science, University of Waikato, New Zealand. At the Cyber Security Lab, he was involved with the user-centric security and privacy paradigms. Before joining the University of Waikato, he worked as a Senior Research Fellow at Edinburgh Napier University. During his work at the Edinburgh Napier University, he worked on the RatTrap project. The RatTrap project was involved in designing a suite of preventive technologies to avoid online fraud—especially in the online affiliate marketing. Raja obtained his Ph.D. in Information Security from Royal Holloway, University of London. He completed his M.Sc. Information Security at Royal Holloway, University of London in September 2007. He also has an M.Sc. Computer Science from University of Agriculture, Faisalabad and B.Sc. (Mathematics, Physics and Geography) from University of the Punjab, Lahore. His research interests revolve around the user-centric applied security and privacy architectures, especially in the field of smart cards, and data provenance in a heterogeneous computing environment. In addition, he is also interested in smart card security, secure cryptographic protocol design and implementation, smartphone security, trusted platform architecture and trusted/secure execution environment.

Tony Boswell began working in IT security as a security evaluator in one of the original UK government Evaluation Facilities in 1987. Since then, he has worked on a wide range of secure system developments and evaluations (including the ITSEC E6 certifications of the Mondex purse and the MULTOS smart card operating system) in the government and commercial domains. Tony has been involved in UK and international interpretation of evaluation requirements for smart cards since 1995 and continues to contribute to multinational technical community work on interpretation and maintenance of Common Criteria evaluation requirements, as well as assisting developers to take their products through Common Criteria evaluations. He is currently a senior principal consultant at DNV GL and technical manager of the DNV GL Technical Assurance Laboratory CLEF.

Joos Cadonau received his B.Sc. in Electronic Engineering and Telecommunication in 1994 from the University of Applied Sciences in Bern, Switzerland. After his degree, he worked as project manager for the primary Swiss Telecommunication provider Swisscom AG in Network Access Management Systems, followed by a project manager role in Ascom AG in the area of PBX switches (Private Branch Exchange). From 2001 until 2011, he acted as Product Manager for Sicap AG, a Swisscom subsidiary, managing SIM-based over-the-air solutions for telecommunication customers all over the globe. During this period, he focused on the role of the SIM card in

complementary security centric services, such as NFC payments, M2M connectivity management platforms and Mobile Identity products. After further engagements for the Swiss Railway company in the area of GSM-R and for Swisscom AG in the Centre of Competence for Machine-to-Machine communication, he joined iQuest Schweiz AG in 2014 to develop Identity and Internet of Things (IoT) offerings.

Sheila Cobourne, MA (Oxon), MBA., M.Sc. read Physics at Lady Margaret Hall, Oxford, and went on to work as a systems analyst developing financial systems for various multinational organisations. She has an MBA from Henley the Management College and a M.Sc. in Mathematics from the Open University. She studied the M.Sc. in Information Security at Royal Holloway, University of London and passed (with distinction) in 2010. She is a Ph.D. student in the Information Security Group Smart Card Centre supervised by Professor Keith Mayes.

Paul Dorey, Ph.D., CISM F.Inst.ISP is a cybersecurity and risk management strategist, who supports company Boards, Executives and CISOs in devising and developing their cybersecurity management capability. He has over 25 years of management experience in digital security and enterprise risk management including information security, digital security of process control/SCADA systems, Business Continuity Planning, privacy and information management. His leadership roles include Global CISO at BP and global leadership of strategy, information security and risk management functions at Morgan Grenfell and Barclays Bank. Paul has consulted to several governments and was a founder of the Jericho Forum and for several years sat on the Permanent Stakeholders Group of the European Network Information Security Agency (ENISA). He was one of the founders of the Institute of Information Security Professionals, and after 5 years as Chairman of the Board, he is now a Fellow of the Institute and Chairman Emeritus. He is also a Visiting Professor at Royal Holloway, University of London.

Claus Ebner born 1962 in Krumbach, Germany, studied mechanical engineering at the Technical University of Munich. Afterwards, he did his doctorate at the Institute for Machine Tools and Industrial Management of the same university. In 1995, he joined Giesecke & Devrient (G&D) in Munich as Head of IT and development in the Card Service Center. After his involvement in the introduction of an ERP system for the card business, he took over responsibility for the international production software development of G&D. This centre provides software for smart card production to the worldwide subsidiaries of G&D and supports the setup of card production or personalisation sites in G&D's solution business as well. He then moved to the Corporate IT of G&D as Head of Enterprise Architecture, working on the standardisation of the global IT landscape. Now, as Head of IT Governance & Architecture at G&D, he is also responsible for managing the business demands and the IT project portfolio.

Tim Evans is an international industry-recognised SIM expert who has delivered many SIM designs and patents for companies including Vodafone and Truphone. Tim is very involved in SIM/UICC/USIM/eSIM standardisation, where he was chair of ETSI SCP REQ and vice-chair of ETSI SCP over 10 years. Tim has trained many operator SIM teams and is currently working for Vodafone R&D. He is Vodafone's 3GPP SA3 and ETSI SCP delegate setting the security standards for 5G, Internet of Things (IoT) and future SIM technologies; the rapporteur of around 30 SIM and security standards and also is the Vodafone eSIM solutions architect.

Thomas Goetz was born 1970 in Neumarkt i. d. OPf., Germany, and studied microengineering at the Georg-Simon-Ohm University of Applied Sciences of Nuremberg. Afterwards, he did his thesis at the R&D Center of Philips Kommunikations Industrie (PKI) in Nuremberg. In 1994, he joined Giesecke & Devrient in Munich as project manager in the card service centre. From 1999 to 2001, he was based at the company's London office for the set-up and integration of a service centre serving the UK market. Then, he took over responsibility for the Munich-based international smart card production support and industrial engineering team. Since 2011, he responds the strategic planning and its deployment for Global Operations of the Mobile Security Business Unit. The unit supplies innovative security solutions for digital applications to financial institutions, network operators, transport providers and businesses in all sectors.

Gerhard P. Hancke is an Assistant Professor at City University of Hong Kong. Previously, he worked as postdoctoral researcher and fellow in the Information Security Group, Royal Holloway, University of London. He obtained M.Eng. and B.Eng. degrees from the University of Pretoria (South Africa) in 2002 and 2003, and a Ph.D. in computer science with the Security Group at the University of Cambridge's Computer Laboratory in 2008. His research interests are system security, embedded platforms and distributed sensing applications.

Danushka Jayasinghe obtained his B.Sc. (Hons) in Computer Networking from the University of Greenwich. He completed his M.Sc. in Information Security (with Distinction) at the Information Security Group, Royal Holloway, University of London, in 2013. He joined the Smart Card Centre to follow a Ph.D. under the supervision of Professor Konstantinos Markantonakis. His research interests are on modern electronic payment systems with the consideration of security, privacy and efficiency of the underlying payment protocols and platforms. He is also interested in alternative payment schemes other than conventional card-based payment methods including digital cash and anonymous and fair-exchange payment protocols.

Ingo Liersch entered the smart security industry in 2001 when joining Giesecke & Devrient GmbH (G&D). As a Product Manager he focused on Government electronic identity cards including smart card operating systems and applications. In

2004, his role changed to a project manager. He was in charge of eID and eHealth Card projects in Europe and Asia. From 2007 until 2013, he was responsible for segment marketing in the G&D Division Government providing solutions for secure government documents. His work included presales, business consultancy, market intelligence and marketing communication for the business segments identity and health care. Furthermore, he was responsible for emerging products such as encrypted mobile phones and brand protection systems. Ingo joined Infineon in the Business Line Government Identification in 2014. He is responsible for Product Marketing for the Infineon microcontroller platforms for electronic documents such as ePassports, eIDs or eHealth cards.

Ingo has many years of experience in secure identification and authentication, and together with his team he has become a trusted adviser to governments. Ingo holds a degree in Electrical Engineering and in Industrial Engineering. He is active in the Smart ID industry and participates in various industry organisations. Ingo represents Infineon in Silicon Trust (www.silicon-trust.com). Ingo gives lectures on electronic passports and ID cards at Royal Holloway, University of London (Information Security Group Smart Card Centre). Furthermore, he is well known in the smart security market due to publications and articles in identity journals.

David Main began his career as an electronic engineer in the late 1970s and progressed with a number of companies from guided weapons, through process control, to passport and fingerprint systems. Highlights included working with the first 16-bit microprocessors and a contactless electronic coin. In the early 1990s, he moved to Visa and became involved with chip technology from the inception of EMV and developed personally in the areas of cryptology and information security. EMV focus topics included: chip to terminal security architecture, Level 1 communications, contactless (including NFC/mobile) and supporting standardisation ISO & European. David now runs a small independent consultancy specialising in payment industry technology and security. His interests include travel, gardening, golf and in particular vintage car restoration.

Damien Sauveron received his M.Sc. and Ph.D. degrees in Computer Science, from the University Bordeaux 1, France. He is Associate Professor with Habilitation at the XLIM laboratory (UMR 7252 University of Limoges/CNRS France) since 2006. He is Head of the Computer Science Department of Faculty of Science and Technology of University of Limoges. Since 2011, he is a member of the CNU 27, the National Council of Universities (for France). Since 2014, he is chair of IFIP WG 11.2 Pervasive Systems Security and was vice-chair before.

His research interests are related to Smart Card applications and security (at hardware and software level), RFID/NFC applications and security, mobile networks applications and security (especially Unmanned Aerial Vehicle (UAV)), sensors network applications and security, Internet of Things (IoT) security, Cyberphysical Systems security and Security Certification Processes. In December 2013, the General Assembly of IFIP (International Federation for Information

Processing) has granted him the "IFIP Silver Core Award" for his work. He has been involved in more than 100 research events in different positions (PC chairs, General Chair, Publicity Chair, Editor/Guest Editor, Steering Committee Member, Program Committee Member, etc). At the time of writing, he is involved in more than 5 funded projects on security of UAV fleets.

Chris Shire has a background in security technologies and semiconductor hardware. He joined Infineon (then Siemens) Chipcard & Security business line in 1998, with many years of experience in the industry. His current focus of activity is with projects in the embedded, mobile, transport and payment sectors. He is active in helping to set standards for the UK and establish new security solutions. Chris is an active member of the Institution of Engineering and Technology (IET), UK Smart Card Club, and has been a guest lecturer for several years on the Royal Holloway, University of London M.Sc. course for Smart Card Security. He has written several articles on security technology and contributed to textbooks on the subject.

John Tierney gained his degrees in Pure Mathematics and Computing from Sheffield (B.Sc.) and Numerical Analysis from Liverpool (Ph.D.) Universities. Dr. John Tierney initially worked in communications security, including early ITSEC work in the early 1990s. He has worked with smart cards since 1993, initially developing a secure operating system and applications for prepaid phone card. He joined Mondex in 1999 and worked on a series of Common Criteria and ITSEC evaluations on a range of smart card products. Since 2002, he was worked for MasterCard providing support to banks who implement chip, contactless and mobile payment technologies. He lives in Wirral.

Allan Tomlinson received a B.Sc. in Applied Physics from the University of Strathclyde in 1981; M.Sc. in Microelectronics in 1987 and doctorate in 1991, both from the University of Edinburgh. His thesis was on "VLSI architectures for cryptography". He then joined the Institute of Microelectronics at the National University of Singapore, working on secure NICAM broadcasting and video compression. In 1994, he moved to General Instrument in California to work on the Digicipher II Conditional Access system for digital video broadcasting. Before joining the Information Security Group at Royal Holloway, he was Principal Engineer at Barco Communications Systems where he was responsible for the development of the "Krypton" DVB Video Scrambler. He also served for a number of years on the DVB Simulcrypt committee. His current research interests are distributed systems security, trusted computing and mobile network security.

Chris Torr joined the MULTOS Consortium, MAOSCO Ltd, as technical manager in 2012 bringing with him eleven years' experience in smart cards. His career has also spanned the electronics and defence industries. It has taken him around the world promoting, developing and deploying solutions and providing training.

He has a B.Eng. Honours degree in Information Systems Engineering from Coventry University.

Michael Tunstall has been working in embedded security since 1998, primarily focused on side channel and fault analysis of cryptographic devices. He started his career in Gemplus Card International, the world's leading smart card maker, and was involved in the development of side-channel attacks and countermeasures, from the moment it was introduced to the cryptographic community as a very real security issue. He is also responsible for some of the first publications demonstrating that fault analysis of cryptographic devices is possible and that suitable countermeasures are required in all such devices. He has coedited a book entitled "Fault Analysis in Cryptography", which is a summary of the state-of-the-art in fault analysis and is the first text book on this topic in the literature.

Assad Umar received his B.Sc. in Business Information Technology from Coventry University UK in 2010 and his M.Sc. in information security from Royal Holloway in 2012 with a distinction. Prior to joining the Information Security Group as an M.Sc. student, he worked for a year in the Information Security Department of the Nigerian Communications Commission NCC. His research interests include smart cards, Near-Field Communication, smartphone security, transport ticketing, network security and security architectures. He is a Ph.D. student in the Smart Card Centre conducting research in transport ticketing systems under the supervision of Professor Keith Mayes on a project funded by Transport for London.

Gary Waite is the executive director—embedded SIM, Connected Living at GSMA. In the early 1990s, Gary designed and sold what became the de facto standard SIM and mobile test tool for the entire GSM industry via a start-up attracting $20m of venture capital funding to enhance SIM card security. Gary spent over ten years with Telefonica, advising on key technology areas such as SIM, location and Machine-to-Machine (M2M). His recent work has made the GSMA Embedded SIM specification the de facto standard for the M2M industry, and today, he is playing a key role in the development of remote SIM provisioning for consumer devices.

Anjia Yang is a Postdoctoral Fellow in the Department of Computer Science at City University of Hong Kong, where he obtained his Ph.D. in 2015. He visited I2R, A*STAR, Singapore (2013–2014), and Chalmers University of Technology, Sweden (2014), respectively. His research interests include RFID security and privacy, Security of Internet of Things, Cloud Security and Cryptographic Protocols.

List of Figures

List of Tables

List of Reviewers

Keith Mayes
Konstantinos Markantonakis
Raja Naeem Akram
Tony Boswell
Sheila Cobourne
Paul Dorey
Thomas Goetz
Gerhard Hancke
Danushka Jayasinghe
Ingo Liersch
David Main
Damien Sauveron
Chris Shire
Allan Tomlinson
Chris Torr
Michael Tunstall
Assad Umar
Anjia Yang