Secure Smart Embedded Devices, Platforms and Applications

Konstantinos Markantonakis
Keith Mayes
Editors

Secure Smart Embedded Devices, Platforms and Applications

Foreword by Fred Piper

Springer

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

ISBN 978-1-4614-7914-7 ISBN 978-1-4614-7915-4 (eBook)
DOI 10.1007/978-1-4614-7915-4
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013939824

© Springer Science+Business Media New York 2014
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

I would like to dedicate this book to the memory of my father, Georgios Markantonakis. Thank you dad!

Konstantinos Markantonakis

I would like to dedicate this book to my family and friends, and to people who succeed despite disadvantage

Keith Mayes

Foreword

This is the second book to be co-edited by Keith Mayes and Konstantinos Markantonakis. The first, *Smartcards, Tokens, Security and Applications* was published in 2008 and this volume is a natural ‘companion’ of that earlier publication and greatly expands on the range of content. Both are the result of experiences gained in managing the Smart Card Centre (SCC) at Royal Holloway, University of London.

The SCC, which was founded 10 years ago by Vodafone and Giesecke & Devrient, and has since been supported by numerous other companies, teaches a specialist module to students studying for the M.Sc. in Information Security. That module, which has the same title as their first book, focuses strongly on the relevant technical, practical and security issues.

Just as with the earlier book, the editors have produced an informative volume that is easy to read and its wide range of topics, which includes RFID, NFC, Mobile communications and wireless sensor nodes, (to list only a few), will appeal to a much wider audience than the Masters students at whom it is primarily aimed. This wider audience is likely to extend to researchers and experts form industry and governments. The two editors are both active researchers and their enthusiasm for research adds extra interest to a fascinating area.

It is clear that technology has advanced enormously over the years, although the fundamentals of Information Security may not have changed very much. Whether we are dealing with pencil and paper or advanced super computers, the motivation for fraud or security attacks and many of the reasons why vulnerabilities exist still have very human origins. Perhaps the biggest change is that people have transformed from being occasional users of technology to being dependent upon it and its underlying security properties. We also have generations that have grown up with the computer, mobile phone and Internet connectivity as essentials for life and they consume services and share personal data with carefree enthusiasm, whereas older heads might worry about how the technology works, who controls the system and data etc. In response to this it is certainly possible to focus on the security of something “big” like the Internet, but is very important to remember that much of what we rely on to keep us and our data and activities secure, is a collection of increasingly complex smaller devices. For example, the mobile phone is really a concept and what we actually buy and use is an electronic assembly with processors, memories, security modules, displays, batteries, speakers etc. We could almost describe a car in the same way as it only functions correctly because a large number of embedded electronic modules, processors, sensors and communications links work as they should. Therefore if we are to fully understand the threats to modern systems and services, and then to help protect against them, we should keep abreast of developments in embedded systems. A textbook on secure smart embedded devices, platforms and applications would therefore seem a welcome addition to the bookshelf.

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

Preface

As we progress into the twenty-first century it seems that the pace of technological advance shows no sign of slowing. We are in fact becoming increasingly dependent on technology in our normal day-to-day lives, which means that we are critically reliant on the security of systems and services that are built upon this technology. In exploring this issue within a textbook, one could consider the high-level design aspects or concentrate more on the nuts and bolts of security systems. This book focuses mainly on the latter approach, as the editors and authors felt there was no introductory overview that covered a sufficient breadth of available technology and related issues. Generally speaking, a complex system is made up of smaller components such as devices, processors, security modules, memories etc. and knowing which of these can be trusted (and to what extent) to resist attacks and misuse, is critical to the security of the complete system. For example, a very sophisticated and expensive car might be reliant on a tiny embedded device (chip) in the engine management system, for it to start and for protection against theft. It is hoped that this book will help to clarify the role of embedded devices, their capabilities, and how best to exploit them in secure system designs.

Structure of the Book

The book consists of 24 chapters organised in four sections. Part I introduces some typical embedded devices and hardware, before some more generic information on security issues is provided in Part II. The Part III (which is the largest section) considers a wide range of application aspects and considerations. Part IV is provided for readers who are interested in application development for embedded devices. The chapters are written as self-contained texts, from a range of expert authors and can be read individually or in the book order. The chapters are briefly introduced below.

Part I: Chapter 1 provides an overview of smart cards and (RFID), their security capabilities and attack resistance, and their widespread use within a range of security sensitive applications. Chapter 2 then introduces Digital Signal Processor devices which are widely used in modern devices, such as mobile phones. Chapter 3 relates the historical development of microprocessor and microntroller chips and goes onto cover the specialist design of secure embedded microcontrollers. Chapter 4 introduces a specific type of secure controller, the Trusted Platform Module (TPM) and its mobile equivalent, that are intended to ensure (amongst other things) the safe boot up of a computing platform, so it is a reliable platform on which to load applications. Chapter 5 considers the Very Large Scale Integration (VLSI) approach to the design of electronic hardware and the potential for security attacks and associated countermeasures.

Part II: Chapter 6 provides a general recap on information security best practices. Although we are focussing on embedded devices we must not forget that without a secure theoretical design the implementation security will be fundamentally flawed. Chapter 7 illustrates how a theoretically sound security design can be undermined by a poor implementation that lacks attack resistance. The chosen attack target is the smart card; however the principles are applicable to most embedded security devices. Chapter 8 considers the Graphics Processing Unit (GPU), a processing platform that is often overlooked for its security capabilities. It can be used as a cryptographic processor; however it is also a target for malware and general misuse. Chapter 9 focuses on the FPGA, which has been exploited both to protect and to attack security systems. The discussion also extends to the protection of valuable Intellectual Property loaded into FPGAs used in commercial systems.

Part III: Chapter 10 considers a range of options for providing mobile communications security controllers. It begins with the conventional Subscriber Identity Module (SIM) and the associated personalisation, management and usage processes, but goes on to consider other possibilities, including software SIMs and TPMs. The action taken by a mobile device depends not just on the security controller, but the validity of the data that it receives, which increasingly can include a representation of physical location. Chapter 11 discusses practical approaches to location estimation, highlighting the possible security vulnerabilities. Car Satellite Navigation systems are just one obvious example of this; however as discussed in Chap. 12 motor vehicles are packed with processing technology that has important safety and security aspects. By contrast, payment card systems tend not to have such emphasis on safety, but they are required to safeguard significant financial transactions. The potential to undermine the payment terminals is discussed in Chap. 13 with reference to published attacks. Another technology where the misuse may have both safety and security implications is the (WSN) which is described in Chap. 14. For example, if a sensor value is modified, replaced or blocked the resulting effect could be serious and/or costly if the system was used for say telemedicine or metering. In fact a number of sensing and terminal solutions are proposed around mobile devices and this seems to be expanding with the arrival of (NFC) Technology. Chapter 15 considers NFC and its security in detail, and how the phone (or laptop, PDA, tablet) may emulate an RFID, or act as an RFID reader, or communicate with other NFC phones over a close proximity link. Although NFC includes a Security Element (SE) some aspects of the functionality are reliant on the phone platform security, which has vulnerabilities similar to conventional PCs. To clarify this problem, Chap. 16 provides a recap on BIOS and Rootkit infections on computing platforms. Specialist computing/server equipment can get around this problem to some extent by the use of security hardened peripheral devices for sensitive processing. These are commonly known as Hardware Security Modules (HSM), and are discussed in Chap. 17. Such devices are normally required to be formally security evaluated and the Common Criteria approach to this is outlined in Chap. 18. In Chap. 19 there is a description of Physically Uncloneable Functions (PUFs) that have generated significant academic interest and then in Chap. 20 there is an overview of SCADA systems security that has generated significant industry concerns.

Part IV: Chapter 21 provides an overview of the PIC family of microcontrollers that are intended for general-purpose non tamper-resistant implementations; however they are often used as clone platforms, as well as for research experiments. More secure implementations are commonly implemented on Java Card platforms and the programming aspects are introduced in Chap. 22. Java has also been a preferred approach for mobile phone platforms and this approach plus important APIs are described in Chap. 23. Finally, for readers interested in experimenting with Wireless Sensor Nodes, some practical guidance on available platforms is presented in Chap. 24.

The ISG Smart Card Centre
Royal Holloway, University of London
www.scc.rhul.ac.uk; www.isg.rhul.ac.uk

Keith Mayes
Konstantinos Markantonakis

ISG Smart Card Centre—Members Message

The (SCC) was established more than 10 years ago at Royal Holloway, University of London. The primary objective was to create a World-Wide Centre of Excellence for training and research in the field of Smart Cards, applications and related technologies. Over the years this has expanded into RFID, NFC, mobile devices and general embedded/implementation system security. Following the success of its first textbook in 2008 (Mayes and Markantonakis (eds), *Smart Cards*, *Tokens*, *security and Applications*, Springer) it was felt that this new book was now needed to cover more aspects of Secure Embedded Devices.

The SCC is part of the World renowned Information Security Group (ISG) that is one of the oldest and largest such groups and is one of the UKs Cyber Security Academic Centres of Excellence, with alumni of over 2,000 M.Sc./Ph.D. postgraduates. The SCC in common with ISG principles is very strongly engaged with industry, focussing on responsible research into real world projects of significant impact, and actively engaging industry experts into postgraduate training, research and publication.

As representing the range of supporting industrial members, we are pleased to be associated with the work and publications of the SCC.

Orange Labs (UK)
Transport for London
UK Cards Association
ITSO

Acknowledgments

This book would not have been possible without the help and support of a number of organisations and individuals. Firstly we would like to thank Orange Labs (UK), Transport for London, The UK Cards Association, ITSO and Royal Holloway, University of London for their tremendous support of the ISG Smart Card Centre. We owe an enormous debt of gratitude to all chapter authors and reviewers for their expert contributions and patient co-operation. We would also like to extend our thanks to Fred Piper for writing the foreword. Last, but certainly not least, we must thank Raja Naem Akram for his tremendous efforts in helping to bring this book to print and to Sheila Cobourne for proof reading on an epic scale.

Contents

Part IV Practical Examples and Tools

Contributors

Raja Naeem Akram received B.Sc. from University of Punjab, Pakistan in 2002. After graduating, he studied for M.Sc. Computer Science from University of Agriculture, Pakistan. In 2004, after completing the Master's course in Distinction he worked as IT/Computer Science teacher at Government M.C. High School, Samanabad. He completed his M.Sc. Information Security from Royal Holloway, University of London (RHUL) with Distinction in 2007. In 2012 he completed his Ph.D. under the supervision of Dr. Konstantinos Markantonakis. Worked as Senior Research Fellow on the RatTrap project, designing fraud detection techniques in on-line affiliate marketing at Edinburgh Napier University. Currently, working as a Research Fellow at the Cyber Security Lab, Department of Computer Science, University of Waikato, New Zealand. His research mainly focuses on user centric security and privacy models in different computing environments.

Dr. Jérémie Albert received his M.Sc. in Computer Science from the University of Bordeaux in 2007 (with honors). Next, he pursued a Ph.D. in Computer Science in this same University under the supervision of Prof. Serge Chaumette. During his Ph.D. he designeda process calculus suitable for the modeling of Highly Mobile Ad Hoc Networks. After his graduation (with highest honors) in 2010, he was an Assistant Professor at the Polytechnic Institute of Bordeaux. Since 2011, he is a Senior Solutions Architectat Ezakus, Bruges, France. His current research interests are related to distributed computing, large datasets processing, semantic computing, machine learning and game theory.

Dr. Lionel Barrére is the Director of Research and Development team at H5 Audits. He previously graduated from the University of Bordeaux, France, and then received his Ph.D. in2009 under the supervision of S. Chaumette for his work on services over military MANets (Mobile Ad hoc Networks), work that was funded by the DGA (French Army). At the end of 2008, he joined the H5 Audits company to create its R&D Department. His research areasare oriented towards the development of passive network monitoring tools such as network probes.

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 certificationsof the Mondex purse and the MULTOS smart card operating system) in the government and commercial domains. Much of Tonys recent work has been on integrated circuit security projects and on server and application-level virtualisation. Tony has been involved in UK and international interpretation of evaluation requirements for smart cards and payment terminals since 1995, and continues to contribute to multi-national technical community work on interpretation and maintenance of Common Criteria evaluation requirements, as well as assisting hardware and software developers to take their products through Common Criteria evaluations. He is currently a Principal Consultant and CLEF Technical Manager at SiVenture (www.siventure.com).

Serge Chaumette is a Professor in Computer Science at the University Bordeaux 1, Leader of the Mobility, Ubiquity, and Security research group at Laboratoire Bordelais de Recherche en Informatique. He has been using the Java technology for distributed programming since its early beginning. Being concerned by security issues he participated in thedesign of tools to help in the process of evaluating Java Cards (and applications) within government funded industrial projects. He then naturally moved to the domain of mobile systems and networks and he is collaborating with the French Army in the area of MANets; his group is designing peer to peer applications to support battlefield/emergency situation management (fleets of mobile terminals, robots, or drones). He is an expert by the European Union for Framework Program 7 (FP7) and non FP programs, expert by the ANR (French National Research Agency), and expert by the AERES (French Research and Higher Education Evaluation Agency). He is a member of IEEE, of IEEE Portable Information Devices (PID) group, of Situation Management SubCommittee of the Communications and Operations Technical Committee of the IEEE Communication Society, of IFIP groups 8.8 Smart Cards and 11.2 Pervasive Systems Security.

François Durvaux is a Ph.D. Student at Universit Catholique de Louvain. He received the Electro-mechanical Engineering Science degree from UCL in 2010 with his master thesis under the supervision of Pr. Jean-Didier Legat. He joined the Pr. Legat's team in October2010 to work as a researcher in the field of digital nanoelectronics. In January 2011 he started a Ph.D. thesis in cryptography under the supervision of Pr. Franois-Xavier Standaert at UCL. His researches are currently focused on cryptographic hardware design, side-channel analysis, and intellectual property protection.

Dr. Igor Nai Fovino Igor is the Head of the Research Division of the Global Cyber Security Center. Igor has deep knowledge in the fields of ICT Security of Industrial Critical Infrastructure, Energy and Smart Grids, Risk Assessment, IDS, Cryptography. He is author of more than 60 scientific papers published on international journals, books and conference proceedings; moreover, he serves as reviewer for several international journals in the ICT security field. In May 2010 he received the IEEE HSI 2010 best paper award in the area of SCADA Systems. He is also an expert in European Policies (mainly in CIIP field). From 2012 he is member of the European Commission Experts Working Group on the security of ICS and Smart Grids. During his career Igor worked as Contractual Researcher at the University of Milano in the field of privacy preserving datamining and computer security and as Contractual Professor of Operating Systems at the University of Insubria. From 2005 to 2011 he served as Scientific Officer at the Joint Research Centre of the European Commission, providing scientific support to the EU Policies related to the EPCIIP program. Since 2007 he is member of the IFIP Working Group on Critical Infrastructure Protection.

Lishoy Francis is a Security Researcher with background in Computer Science and Engineering, and has specialised in Information Security. In 2002, he graduated with a B.E. in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belgaum, India. In 2004, he graduated with a M.Sc. degree in Information Security from Information Security Group (ISG) at RHUL. He is currently in his final stages of a Ph.D. degree in Information Security at RHUL. He has extensive practical experience in security testing and product prototyping of smart card, mobile, location, contactless, RFID and proximity technologies. He is an acknowledged and published expert on NFC security. He started his career by working as a Software Engineer in Wipro Fluid Power LTD (Wipro Group), Bangalore, India; and more recently he worked as an Expert Consultant at Crisp Telecom UK LTD. He is currently employed as a Senior Research Engineer at France Telecom R&D UK LTD (Orange, UK) where he is enterprising excellence and innovation in information security.

Dr. Mick Ganley is an independent security consultant who has worked in the industry for 25 years. He specialises in the security of card payment systems, cryptography and key management, hardware security modules and security management. His current client list includes a number of the worlds largest multinational corporations. Until recently, he provided consultancy services to the prestigious ISG at RHUL, and was on the editorial board of the Information Security Technical Report, published jointly by the ISG and Elsevier. In previous lives he was an academic mathematician and Head of Security Analysis for the security division of Racal (now Thales).

Univ.-Prof. DI Dr. Thomas Grechenig is a Senior Architect in large IT systems and nation-wide IT-infrastructures. He is a Professor for Industrial Software Engineering at the Vienna University of Technology. He and his teams have planned, designed, and built several large scale NFC-solutions in payment, mobile keys, mobile ticketing, railway and public transport applications. In science and research the focus of interest goes towards (a) enhancing the stability and fine-tuning of the NFC-mass-concept in all its critical sectors (usability, security, IT-infrastructure, performance, integration and interoperability) (b) redefining every day use cases and interactions for the consumers via NFC in a way that preserves the users' old experiences while providing "the new ubiquitous feeling of simple touch interaction" in a natural form (c) this leads into a science aiming at re-understanding daily processes like payments, locking doors, showing tickets, or personal identification in its newly adapted "Gestalt" in fusion of the old metaphors, new facilities as well as its privacy and security needs. From a more abstract scientific point of view Thomas Grechenig promotes NFC being one out of 5 major technology enablers towards a "vitalized" environment on all three relevant operative levels: (1) "desktop"/individual (2) buildings/groups (3) urban and regional/social.

Dr. Gerhard Hancke (B.E., M.E., Ph.D., CSCIP, SMIEEE) received a Bachelor and Masters of Engineering degrees in Computer Engineering from the University of Pretoria (South Africa) in 2002 and 2003, and a Ph.D. in Computer Science for the Security group at the University of Cambridge's Computer Laboratory in 2008. He joined the ISG in 2007 as a post-doc, working within the ISG Smart Card Centre managing the RFID/Contactless research track and RF/Hardware laboratory. In 2011, he was appointed as a Fellow within the ISG. His main interests are smart hardware tokens and their applications, mobile systems and pervasive computing.

Graham Hili B.Sc. I.T. Hons (Malta), M.Sc. (Royal Holloway) began his career with the Vodafone Group (Malta) where he was in charge of the security and the availability of the mobile value added systems (SMS, MMS, WAP). After this he moved to a consultancy position with Orange Group in The Netherlands. His current fields of specialisation include smart card security and the development of digital identity and digital security in IT systems and virtual worlds.

DI Christian Kantner graduated in Communications Engineering from the Vienna University of Technology in 1997 Christian Kantner joined Ascom Business Systems in Switzerland. He was responsible for the design and implementation of data and fax protocols for the Thuraya satellite phone system. Before he joined Mobilkom Austria in 2003 he was working as Freelancer for Ascom (Solothurn), Philips Semiconductors (Zurich) and Hughes Network Systems (San Diego, CA) in the field of GSM and Data Protocols. He taught Real Time Operating Systems for several years at the University of Applied Science in Upper Austria. In 2003 he joined Mobilkom Austria's TechLab, where he was responsible for analyzing new technologies for mobile phone operators, focusing mainly on mobile terminal technology. He has been investigating NFC technology since 2004 and got involved in NFC Forum activities in 2005. He is coeditor of the NFC technical guidelines white paper published by the GSMA. Christian Kantner joined Mobilkom Austria's m-commerce team as Product Manager for NFC in 2007. He was in the leading team for key NFC projects at Mobilkom Austria. From 2010 to 2012 Christian Kantner was head of IT and Services at Mobilkom Austrias daughter paybox Bank. Paybox Bank operates ad hoc mobile payment services for customers of A1, T-mobile Austria and Orange Austria. Christian Kantner has dedicated his career to wireless communications. Starting with 36,000 km satellite links and arriving at 3 cm NFC transactions. He has deep understanding about technological aspects as well as market insight. Christian Kantner is now driving the payment innovation roadmap in A1 Telekom Austria (former Mobilkom Austria).

Stéphanie Kerckhof is a Ph.D. student at Universit Catholique de Louvain. She received the Electro-mechanical Engineering Science degree from UCL in 2007 with her master thesis under the supervision of Pr. Jean-Didier Legat. She was a hardware developer for two years at intoPIX, Louvain-la-Neuve, Belgium. In April 2010, she started a Ph.D. thesis in Cryptography under the supervision of Pr. Franois-Xavier Standaert at UCL. Her researches are currently focused on cryptographic hardware design, side-channel analysis, and intellectual property protection.

Mario Kirschbaum received the B.Sc., M.Sc., and Ph.D. degrees in Telematics from Graz University of Technology in Austria, in 2005, 2007, and 2011, respectively. He is currently working as a member of the Secure Entities for Smart Environments (SEnSE) group of the Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria. His research interests include implementation attacks, development and investigation of countermeasures, and the implementation of cryptographic hardware modules.

Dr. Gerald Madlmayr is an IT and Telecommunication Architect based in Vienna. In his daily work he is confronted with technology strategy for mobile network operators, software system and IT Integration in banking and payment systems as well as customer focused mobile technologies and devices. Besides that, he is Lecturer at the Vienna University of Technology at the Research Group for Industrial Software. There his research is focused on mobile technology in society as well as energy and environmental topics. Before that he worked as a Research Associate at the Research Center Hagenberg. There his work was focused on NFC/RFID based applications as well as security and privacy in such systems. He is an authority on NFC technology and applications, actively participating in the standardization of NFC. Within the scope of this job one of the most sophisticated NFC trials was launched in 2006. Previously Gerald Madlmayr was working as a visiting Researcher in Princeton/New Jersey at Siemens Corporate Research (SCR) dealing with the design and implementation of CSCW Systems. Before that he was part of the innovations department of Siemens mobile in Munich. There he also wrote this diploma thesis with the focus on image processing on mobile devices. Gerald Madlmayr holds a Diploma in Media Technology from the University of Applied Sciences of Hagenberg and a Ph.D. in Computer Science from the University in Linz.

Konstantinos Markantonakis B.Sc. (Lancaster University), M.Sc., MBA, Ph.D. (London) received his B.Sc. (Hons) 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 RHUL. He is currently a Reader (Associate Professor) in the ISG. His main research interests include smart card security and applications, secure cryptographic protocol design, Public Key

Infrastructures (PKI) and key management, embedded system security, mobile phone operating systems/platform security, NFC/RFID security, grouping proofs, electronic voting protocols. 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 a Multi-application Smart Card Manager in VISA International EU, responsible for multi-application smart card technology for southern Europe. More recently, he was working as a Senior Information Security Consultant for Steer Davies Gleave, responsible for advising transport operators and financial institutions on the use of smart card technology. He is also a member of the IFIP Working Group 8.8 on Smart Cards. He has published more than 90 papers in international conferences and journals. 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.

Stathis Mavrovouniotis was born in Athens, Greece on June 27th, 1981. Stathis attended the Athens University of Economics and Business (AUEB) and graduated in 2004 with a degree in Business Administration. Following his graduation from AUEB, Stathis attended the RHUL and received two M.Sc. degrees, in Business Information Systems (2005) and in Information Security (2006). After serving his military service back in Greece, he was offered the job of IT Security Analyst in First Data Greece International, having the main responsibilities of key management, compliance, audit preparation and Incident Investigation/Report as well as Implementation of security related tools. Stathis soon became the IT Security Manager for SE Europe, Middle East and Africa in First Data International, focusing in implementing the information security policy and addressing it with procedures and guidelines, maintaining compliance with payment schemes, PCI DSS and ISO 27001, running IT Security related audits and gap analysis, security planning, risk assessments and implementation of security awareness programs. He has been also assist in consulting and assessments around key management in different First Data sites. He has been so far qualified with the following certifications: CISM, SSCP, ISO 27001:LA, PCI ISA, CTGA and is member of ISC2, ISACA and active member of the local OWASP chapter.

Keith Mayes is the Director of the Information Security Group-Smart Card Centre (ISG-SCC) (www.scc.rhul.ac.uk) at RHUL. He is also the Founder and Managing Director of the consulting company Crisp Telecom Limited (www.crisptele.com). He is currently a non-executive independent Director of AIMs listed GMO ltd., a provider of mobile services in China and a Director of IWICS Europe Limited, a 4G mesh radio network company. Dr. Mayes has a Bachelor of Science degree in Electronic Engineering and a Ph.D. in Digital Image Processing from the University of Bath. He is a Chartered Engineer and Member of the Institute of Engineering and Technology. He is also a Member of the Licensing Executives Society and a Founder Associate Member of the Institute of

Information Security Professionals. During a long and varied industry career he has worked for Philips, Honeywell Aerospace & Defence, Racal Research and finally for the Vodafone Group as the Global SIM Manager responsible for SIM card strategy and harmonisation. Aside from his current research and teaching focus on smart cards, RFIDs and security, he has maintained an active interest in mobile communications, hardware and software development, Intellectual Property and radio relay trials.

Mehari G. Msgna received a Bachelor of Engineering degree in Electronics and Communication Engineering from Mekelle Institute of Technology (Ethiopia) in 2007. In 2009 he received a Masters of Science degree in Information Security from RHUL and he started his Ph.D. with the ISG in 2011 at the same institution. His research interests are virtual machines for embedded devices, smart cards/tokens security, biometrics and side channel analysis.

Jan Pelzl Since 1994, Dr. Pelzl works in the area of IT-security. In 1997, he received the certificate as telecommunication technician from the company Bosch Telecom. Since 1999, Dr. Pelzl is working in the area of embedded IT-security. He successfully accomplished many national and international projects and released numerous related publications at renowned international conferences and in journals. As a researcher, Jan Pelzl investigated practical aspects of elliptic-curve-based cryptography and cryptanalysis. Dr. Pelzl is teaching data security and introduction to cryptography for industry courses, e.g. for TV-Akademie Rheinland, gits AG and Ruhr-University of Bochum. From March to August 2007, Dr. Pelzl was Chief Technology Officer (CTO) of ESCRYPT GmbH. Since September 2007, Dr. Pelzl is Managing Director of ESCRYPT GmbH.

Thomas Plos received the B.Sc. and M.Sc. degrees in Telematics from Graz University of Technology (TU Graz) in 2004 and 2007, respectively. In 2011 he received the Ph.D. degree in Computer Science from TU Graz. His research interests include digital VLSI design with a focus on low power and low-area circuit design, information security, RFID technology, and implementation attacks such as side-channel analysis and fault analysis. Currently, he is a post-doctoral researcher at the Institute for IAIK at TU Graz.

Konstantinos Rantos is an Assistant Professor at the Industrial Informatics Department of the Technological Educational Institute of Kavala. He received his Diploma in Computer Engineering and Informatics from the University of Patras, Greece, and both his M.Sc. and Ph.D. in Information Security (sponsored by Marie Curie Research and Training Grant) from RHUL. He has extensive project involvement and substantial (more than 15 years) private- and public-sector experience in the area of information security which he gained while holding positions in both sectors as well as in academia. His scientific interests lie in the areas of public-key infrastructures, embedded systems, e-government services, authentication systems, smart cards, electronic payment systems and security awareness. He is a reviewer to a number of conferences and scientific journals and authored many articles and papers.

Serendra Reddy has earned his B.Sc. in Engineering from the University of Natal and a Masters in Engineering from the University of Pretoria. He is currently completing his Ph.D. in Engineering at the University of Cape Town, South Africa. His doctoral research is involved in the investigation and development of methods for autonomous three dimensional conversion of two dimensional monocular images. Between 1999 and 2005 he worked and consulted for Siemens Telecommunications, having been involved in projects locally and on-location across Africa, the Middle East and Europe. In 2007 he joined the academic staff of the Department of Electronic Engineering at the University of Pretoria, where he lectured on Digital Systems and Digital Signal Processing, and was involved in the Intelligent Systems research group. In 2011 he joined the academic staff of the Department of Electronic Engineering at the Durban University of Technology, where he currently lectures on Radio Engineering. He serves as the Chair of Communications and is a founding member of the Intelligent Systems research group. His research interests include artificial intelligence, machine learning, computer vision, pattern recognition, embedded systems and robotics.

Francesco Regazzoni is a post-doctoral researcher at ALaRI Institute of University of Lugano (Lugano, Switzerland). He received his Master of Science degree from Politecnico di Milano (Italy) and his Ph.D. degree from University of Lugano (Switzerland). He has been a post-doctoral researcher at the Crypto Group of the Universit Catholique de Louvain (Louvain-la-Neuve, Belgium) and has been a visiting researcher at several institutions, including NEC Labs America (Princeton, NJ, USA), Ruhr-University of Bochum (Bochum, Germany), and EPFL (Lausanne, Switzerland). His research interests are mainly focused on embedded systems security, covering in particular side channel attacks, cryptographic hardware, and electronic design automation for security.

Prof. Dr.-Ing. Ahmad-Reza Sadeghi is the Head of the System Security Lab at the Center for Advanced Security Research Darmstadt (CASED), Technische Universitt Darmstadt and the Scientific Director of the Fraunhofer Institute for Secure Information Systems (SIT), Darmstadt, Germany. Since January 2012 he is the Director of the Intel-TU Darmstadt Security Institute for Mobile and Embedded Systems in Darmstadt, Germany. He received his Ph.D. in Computer Science from the University of Saarland in Saarbrcken, Germany. Prior to academia, he worked in research and development of telecommunications enterprises, amongst others Ericson Telecommunications. He has been leading and involved in a variety of national and international research and development projects on the design and implementation of trustworthy computing platforms and Trusted Computing, security hardware, Physically Unclonable Functions (PUFs), cryptographic privacy-protecting systems, and cryptographic compilers (in particular for secure computation). He has been continuously contributing to the IT security research community and serving as general or program chair as well as program committee member of many conferences and workshops in information security and privacy, Trusted Computing and applied cryptography. He is on the Editorial Board of the ACM Transactions on Information and System Security.

Damien Sauveron is Assistant Professor at the XLIM (UMR 6172 University of Limoges/CNRS—France) Laboratory since 09/2004. Damien Sauveron worked during three years for the ITSEF of SERMA Technologies on the Java Card security. During his thesis that he carried out in the Distributed Systems and Objects team of the LaBRI he was one of the main developers of a Java Card emulator, he introduced the concept of pre-persistance in Java Card and he highlighted a new category of attacks on the open multi-application smart cards. From 01/02/2006 to 10/08/2006, he was an invited researcher at the ISG-SCC of the RHUL. He is member of the IFIP WG 8.8 Smart Cards, member of the IFIP WG 11.2 Small System Security and member of IEEE.

Dipl. Ing. Steffen Schulz received his Diploma degree in Information Security from Ruhr-University Bochum, Germany. He works as Research Assistant at the System Security Lab at Ruhr-University Bochum and at the CASED, Technische Universitt Darmstadt, Germany. He currently pursues his Ph.D. in Trusted Infrastructures and Trust Management in a joint cooperation between the System Security Lab in Bochum and Macquarie University Sydney, Australia. Steffen Schulz was involved in several national and international research projects, where he participated in the design and development of trustworthy operating systems, trust establishment in resource-constrained environments and trusted virtualization infrastructures (TVDs). Furthermore, he has worked on different aspects of network security and covert channels, with several publications in international conferences.

Peter Schwabe is a Post-Doctoral Researcher at the Research Center for Information Technology Innovation of Academia Sinica, Taiwan. He graduated from RWTH Aachen University in Computer Science in 2006 and received a Ph.D. from the Faculty of Mathematics and Computer Science of Eindhoven University of Technology in 2011. His research area is the optimization of cryptographic and cryptanalytic algorithms in software. The target architectures of this software range from high-end desktop and server CPUs through parallel architectures such as the Cell Broadband Engine and graphics processing units to embedded processors such as ARM and AVR. He has published articles at several international conferences on fast software for a variety of cryptographic primitives including AES, hash functions, elliptic-curve cryptography, and cryptographic pairings. He has also published articles on fast cryptanalysis, in particular attacks on the discrete-logarithm problem.

Chris Shire has a background in security technologies and semiconductor hardware. He joined Infineon (then Siemens) in 1998 in the Chipcard and Security business line, with many years experience in the industry. His current focus of activity is on projects in the government and finance sectors. He is active on several advisory committees helping to set standards for the UK, and support new security solutions. Chris is an active member of the IET, Intellect, UK Smart Card Club and has been a guest lecturer for several years on the RHUL M.Sc. course on Smart Card Security. He has written several articles on security technology and contributed to textbooks on the subject.

Francois-Xavier Standaert received the Electrical Engineering degree and Ph.D. degree from the Universite Catholique de Louvain, respectively in June 2001 and June 2004. In 2004–2005, he was a Fulbright visiting researcher at Columbia University, Department of Computer Science, Network Security Lab and at the MIT Media Lab, Center for Bits and Atoms. In March 2006, he was a founding member of IntoPix s.a. From 2005 to 2008, he was a post-doctoral researcher of the UCL Crypto Group and a regular visitor of the two aforementioned laboratories. Since September 2008, he is Associate Researcher of the Belgian Fund for Scientific Research (F.R.S.-FNRS) and Professor at the UCL Institute of Information and Communication Technologies, Electronics and Applied Mathematics (ICTEAM). In June 2011, he has been awarded a Starting Independent Research Grant by the European Research Council. His research interests include digital electronics, FPGAs and cryptographic hardware, low power implementations for constrained environments (RFIDs, sensor networks, ...), the design and cryptanalysis of symmetric cryptographic primitives, physical security issues in general and side-channel analysis in particular.

Michael Tunstall has been involved in the research and development on the implementation of cryptographic algorithms on embedded platforms for close to nine years. He was originally employed by Gemplus (now called Gemalto after a merger with Axalto) to develop authentication algorithms for GSM SIM cards. After several years working for Gemplus Michael changed roles within the team to focus on research into attacks and countermeasures that could be applied to smart cards. He was involved in evaluating Gemplus' products to determine whether a suitable level of security had been achieved. The research conducted while Michael was at Gemplus enabled him to start a Ph.D. At RHUL resulting in his thesis entitled "Secure Cryptographic Algorithm Implementation on Embedded Platforms". Michael is currently employed at University College Cork as a postdoctorate researcher, and is currently funded by an Enterprise Ireland grant to develop side-channel countermeasures for FPGA implementations of AES and elliptic curve cryptographic algorithms.

Dipl. Ing. Christian Wachsmann received his Diploma degree in Information Security from Ruhr-University Bochum, Germany. He worked as a Research Assistant at the System Security Lab at the Horst Grtz Institute for IT Security (HGI) at Ruhr-University Bochum. He is currently employed as a Research Assistant at the System Security Lab at the CASED, Technische Universitt Darmstadt, Germany and pursues his Ph.D. on privacy-protecting protocols for mobile and resource constrained embedded devices, in particular RFIDs and smartphones. His work focuses on the development, design and formal modeling of cryptographic primitives and protocols based on physical security features, in particular PUFs. He was and is involved in a variety of national and international research projects and has been continuously contributing to IT security research with several publications at international conferences.

Colin Walter has spent the last 25 years concentrating on the practical implementation of cryptography, partly in industry and partly in academia. He helped design one of the first RSA chips for Plessey-Crypto in 1989. He published the first fully systolic array for modular exponentiation in 1993 and this is now widely used in SSL accelerator chips. In the late 90s he did some consultancy for Multos to understand and reduce side channel leakage from public key cryptography on smart cards. This led to some important work on the implementation of Montgomery modular multiplication and some improved algorithms for exponentiation. He joined the ISG at Royal Holloway in 2009 after 8 years working on product development as head of cryptography at a well-known certificate authority. For many years he was on the steering committee of the IACR CHES workshops, and was programme chair and local organiser for two of these. He is a senior member of the IEEE.

Marko Wolf Dr.-Ing. Marko Wolf is a senior IT security expert and branch manager of ESCRYPT GmbH in Munich. Marko is primarily active in the area of automotive data security and privacy protection for various industry customers in Europe, Asia, and the US as well as for different national and international government authorities and standardization bodies. Marko studied Electrical Engineering and Computer Engineering at the University of Bochum (Germany) and at Purdue University (USA). After receiving his M.Sc. in 2003, he started his Ph.D. in the area of Trusted Computing and vehicular IT security at the Chair for Embedded Security hold by Prof. Dr. Christof Paar. Wolf completed his Ph.D. in 2008 with the first comprehensive work about vehicular IT security engineering. He is editor/author of the books *Embedded Security in Cars* (Springer, 2006) and *Security Engineering for Vehicular IT Systems* (Vieweg+Teubner, 2009), program chair of the international Embedded Security in Cars (escar) workshop series, and has published over 30 articles in the area of embedded IT security and privacy.

Thomas Wollinger Dr. Wollinger has worked in the area of data security and embedded security since 1997. He implemented and led several projects, for instance, at secunet AG. Dr. Wollinger has published numerous articles at international conferences and in relevant journals in the area of security. Dr. Wollinger frequently gives invited talks and teaches data security courses (e.g. at Motorola Labs Paris, gits AG, and TV Academy Rhineland). He obtained his B.S. from the University of Dieburg and obtained his Master of Science at the Worcester Polytechnic Institute, USA. In June 2003, he obtained his Ph.D. with honors from the University of Bochum. Dr. Wollinger worked as Chief Sales Officer (CSO) at ESCRYPT from 2005 to 2007. Dr. Wollinger established the technical sales and marketing structure of the company. He was involved in all acquisitions regarding ESCRYPT projects. Since 2007, Dr. Wollinger is Managing Director of ESCRYPT GmbH.