Smart Card Security And Applications Artech House Telecommunications Library

Future of Trust in ComputingSmart Card Research and
Advanced ApplicationsSmart Card Research and
Advanced ApplicationsSmart CardsSmart Card
ApplicationsSmart Card Application Development
Using JavaSmart Card Research and Advanced
ApplicationsJava on Smart Cards: Programming and
SecuritySmart Card Research and Advanced
ApplicationsJava Card Technology for Smart
CardsPower Analysis AttacksSmart Card Research and
Advanced ApplicationsSmart Card Application
Development Using JavaSmart Card Research and
Advanced Applications VIImplementing Electronic
Card Payment SystemsSmart Card Security and
Applications, Second EditionSmart Card. Research and
ApplicationsSmart Card Programming and
SecurityEmerging Security Algorithms and
TechniquesSecurity and Privacy in the Age of
Ubiquitous ComputingSmart Card Research and
Advanced ApplicationsRecent Trends in Network
Security and ApplicationsRFID and Contactless Smart
Card ApplicationsSmart Grid Applications,
Communications, and SecurityInternet of Things
SecuritySmart CardsSocial and Human Elements of
Information Security: Emerging Trends and
CountermeasuresSmart Card HandbookSmart Card
Research and Advanced ApplicationsSmart Card
SecurityMulti-application Smart CardsSmart CardMulti-
application Smart CardsJava Card for E-Payment

ApplicationsSmart Card Research and Advanced ApplicationsSmart Cards, Tokens, Security and ApplicationsRFID HandbookSmart CardsSmart Card ProgrammingSecure Smart Embedded Devices, Platforms and Applications

Future of Trust in Computing

In the Information Society, the smart card, or smart device with its processing power and link to its owner, will be the potential human representation or delegate in Ambient Intelligence (Pervasive Computing), where every appliance or computer will be connected, and where control and trust of the personal environment will be the next decade challenge. Smart card research is of increasing importance as the need for information security grows rapidly. Smart cards will play a very large role in ID management in secure systems. In many computer science areas, smart cards introduce new dimensions and opportunities. Disciplines like hardware design, operating systems, modeling systems, cryptography and distributed systems find new areas of applications or issues; smart cards also create new challenges for these domains. CARDIS, the IFIP Conference on Smart Card Research and Advanced Applications, gathers researchers and technologists who are focused in all aspects of the design, development, deployment, validation and application of smart cards or smart personal devices.This volume contains the 20 papers that have been selected by the CARDIS Program Committee for presentation at the 6th International Conference on Smart Card

Research and Advanced Applications (CARDIS 2004), which was held in conjunction with the IFIP 18th World Computer Congress in Toulouse, France in August 2004 and sponsored by the International Federation for Information Processing (IFIP). With 20% of the papers coming from Asia, 20% from America, and 60% from Europe, the competition was particularly severe this year, with only 20 papers selected out of 45 very good submissions. Smart Card Research and Advanced Applications VI presents the latest advances in smart card research and applications, and will be essential reading for developers of smart cards and smart card applications, as well as for computer science researchers in computer architecture, computer security, and cryptography.

Smart Card Research and Advanced Applications

Smart cards are currently in widespread use throughout Europe, Asia and South America for making electronic cash, debit and credit payments as well as for a variety of other uses. It is anticipated that within 4 years, over 2.5 billion smart cards will be in use worldwide--with over 25% of that activity expected to be in the U.S. within the next year, smart card pilot programs will emerge in the United States, led by a consortium of banks, telephone companies, transit authorities, the government, and major credit cards. Despite the fact that this new form of commerce is rapidly approaching, very few companies are prepared to make the critical strategic and investment decisions that this revolutionary

technology will demand. Smart Cards: Seizing Strategic Business Opportunities brings readers face to face with the potential impact of the smart card and provides insights on implementing new technologies and innovations. This book helps develop plans, implement solutions and navigate through the myriad investment decisions impacting their introduction and anticipated consumer acceptance of the smart card. Smart Cards will enable the reader to: Develop a model business proposition for introducing a variety of smart card applications' Re-define their markets and their applications, as well as identify potential smart card partners; Minimize the learning curve for launching and implementing a smart card program.

Smart Card Research and Advanced Applications

This book provides readers with an overview to the design of multiapplication smart card environments including the selection of a platform, the creation of applications and the logistics of initial deployment.

Smart Cards

This book constitutes the thoroughly refereed post-conference proceedings of the 17th International Conference on Smart Card Research and Advanced Applications, CARDIS 2018, held in Monpellier, France, in November 2018. The 13 revised full papers presented in this book were carefully reviewed and selected from 28 submissions. CARDIS has provided a

space for security experts from industry and academia to exchange on security of smart cards and related applications.

Smart Card Applications

This book provides a broad overview of the many card systems and solutions that are in practical use today. This new edition adds content on RFIDs, embedded security, attacks and countermeasures, security evaluation, javacards, banking or payment cards, identity cards and passports, mobile systems security, and security management. A step-by-step approach educates the reader in card types, production, operating systems, commercial applications, new technologies, security design, attacks, application development, deployment and lifecycle management. By the end of the book the reader should be able to play an educated role in a smart card related project, even to programming a card application. This book is designed as a textbook for graduate level students in computer science. It is also as an invaluable post-graduate level reference for professionals and researchers. This volume offers insight into benefits and pitfalls of diverse industry, government, financial and logistics aspects while providing a sufficient level of technical detail to support technologists, information security specialists, engineers and researchers.

Smart Card Application Development Using Java

An insightful and practical guide to the use of RFID. The author's professional experience is used to great effect to de-mystify RFID, which is becoming one of the fastest growing sectors of the radio technology industry. Building on Paret's previous technical guide it covers a variety of topics in an accessible manner.

Smart Card Research and Advanced Applications

This book constitutes the thoroughly refereed post-conference proceedings of the 18th International Conference on Smart Card Research and Advanced Applications, CARDIS 2019, held in Prague, Czech Republic, in November 2019. The 15 revised full papers presented in this book were carefully reviewed and selected from 31 submissions. The papers are organized in the following topical sections: system-on-a-chip security; post-quantum cryptography; side-channel analysis; microarchitectural attacks; cryptographic primitives; advances in side-channel analysis. CARDIS has provided a space for security experts from industry and academia to exchange on security of smart cards and related applications.

Java on Smart Cards: Programming and Security

Provides research on the social and human aspects of information security. Presents the latest trends, issues, and findings in the field.

Smart Card Research and Advanced

Applications

This book constitutes the thoroughly refereed post-conference proceedings of the 12th International Conference on Smart Card Research and Advanced Applications, CARDIS 2013, held in Berlin, Germany, in November 2013. The 17 revised full papers presented in this book were carefully reviewed and selected from 47 submissions. The papers are organized in topical sections on security technologies; attacks on masking; side channel attacks; software and protocol analysis; side channel countermeasures; and side channel and fault attacks.

Java Card Technology for Smart Cards

A complete nuts-and-bolts guide to designing, building, and managing the smart card system that's right for your company Already a well-established medium of exchange in Europe, smart card technology has made major inroads in the North American market in the past few years. Visa and Mastercard are committed to replacing credit cards with them over the next five years, and Microsoft is racing to use them for e-commerce. Clearly, the time for asking "Why?" regarding smart cards has passed. The important question companies now should be asking themselves is "How?": how to plan, how to develop, how to implement, and how to manage the smart card system that is right for our company? This book provides complete, unbiased answers to these and all your technical and business questions about smart card systems. Dreifus and Monk guide you step-

Page 7/35

by-step through the entire process of selecting, designing, building, and managing a smart card application tailored to your business. They supply numerous checklists to help guarantee that you make the correct technical decisions during each phase of the process. And they include real-world case studies illustrating successful smart card implementations in a variety of industries, including banking, manufacturing, entertainment, healthcare, and transportation. Crucial topics covered in detail include: * Smart card architectures and standards * Security and encryption * Smart card operating systems * Smart card application design and development * Development tools * Testing and certification Smart Cards arms you with everything you need to know to make informed decisions about the smart card system that's right for your company.

Power Analysis Attacks

The Internet of Things (IoT), with its technological advancements and massive innovations, is building the idea of inter-connectivity among everyday life objects. With an explosive growth in the number of Internet-connected devices, the implications of the idea of IoT on enterprises, individuals, and society are huge. IoT is getting attention from both academia and industry due to its powerful real-time applications that raise demands to understand the entire spectrum of the field. However, due to increasing security issues, safeguarding the IoT ecosystem has become an important concern. With devices and information becoming more exposed and leading to increased

attack possibilities, adequate security measures are required to leverage the benefits of this emerging concept. Internet of Things Security: Principles, Applications, Attacks, and Countermeasures is an extensive source that aims at establishing an understanding of the core concepts of IoT among its readers and the challenges and corresponding countermeasures in the field. Key features: Containment of theoretical aspects, as well as recent empirical findings associated with the underlying technologies Exploration of various challenges and trade-offs associated with the field and approaches to ensure security, privacy, safety, and trust across its key elements Vision of exciting areas for future research in the field to enhance the overall productivity This book is suitable for industrial professionals and practitioners, researchers, faculty members, and students across universities who aim to carry out research and development in the field of IoT security.

Smart Card Research and Advanced Applications

The concept of trust is related to many aspects of our daily lives, and different stakeholders use the term "trust" in various contexts. Trust is crucial in today's information societies for ensuring success of digital economies in all countries and regions. This book contains papers that were presented at the conference "Future of Trust in Computing" and brings together academics, regulators, technologists, and practitioners working in diverse areas of trust from

Page 9/35

various parts of the world. The authors discuss issues they are facing and begin to form a common framework. Security and privacy threats and remedies, core trust-enforcing technologies, innovative applications, regulatory issues, privacy and usability, economics as well as provable security and assurance are discussed. Finally, a number of papers touch upon innovative approaches to trust that begin to define new fields of research and innovative types of technologies.

Smart Card Application Development Using Java

Smart Card Developer's Kit is designed to provide the practical information you need to design and build applications that incorporate smart cards. Using a combination of detailed exposition, technical reference summaries, and extended examples, this book familiarizes you with the unique strengths and capabilities of this emerging computer technology. Increase your security from a one-factor security-a password-to a two-factor security-a smart card and its PIN. Use the smart card as a portable place to carry your personal preference information and your identity-establishing private signing key. In marketing applications, a smart card offers a much wider and more flexible set of customer benefits than a magnetic-strip card or a paper record card. A smart card can also carry secured information-such as medical records, licenses, subscriptions, and accreditations-that must be guarded against tampering.

Smart Card Research and Advanced Applications VI

Smart cards play an increasingly important role in everyday life. We encounter them as credit cards, loyalty cards, electronic purses, health cards, ands as secure tokens for authentication or digital signatures. Their small size and the compatibility of their form with the magnetic stripe card make them ideal carriers of personal information such as secret keys, passwords, customization profiles, and medical emergency information. This book provides a guide for the rapid development of smart card applications using Java and the OpenCard Framework. It gives you the basic information you need about smart cards and how they work. A smart card provided with the book will help you to obtain first-hand experience.

Implementing Electronic Card Payment Systems

Multi-application smart cards have yet to realise their enormous potential, partly because few people understand the technology, market, and behavioural issues involved. Here, Mike Hendry sets out to fill this knowledge gap with a comprehensive and accessible guide. Following a review of the state-of-the-art in smart card technology, the book describes the business requirements of each smart-card-using sector, and the systems required to support multiple applications. Implementation aspects, including security, are treated in detail and numerous international case studies cover identity, telecoms,

banking and transportation applications. Lessons are drawn from these studies to help deliver more successful projects in the future. Invaluable for users and integrators specifying, evaluating and integrating multi-application systems, the book will also be useful to terminal, card and system designers; network, IT and security managers; and software specialists.

Smart Card Security and Applications, Second Edition

Smart Card Security: Applications, Attacks, and Countermeasures provides an overview of smart card technology and explores different security attacks and countermeasures associated with it. It covers the origin of smart cards, types of smart cards, and how they work. It discusses security attacks associated with hardware, software, data, and users that are a part of smart card–based systems. The book starts with an introduction to the concept of smart cards and continues with a discussion of the different types of smart cards in use today, including various aspects regarding their configuration, underlying operating system, and usage. It then discusses different hardware- and software-level security attacks in smart card–based systems and applications and the appropriate countermeasures for these security attacks. It then investigates the security attacks on confidentiality, integrity, and availability of data in smart card–based systems and applications, including unauthorized remote monitoring, communication protocol exploitation, denial of service (DoS) attacks, and so forth, and presents the possible

countermeasures for these attacks. The book continues with a focus on the security attacks against remote user authentication mechanisms in smart card–based applications and proposes a possible countermeasure for these attacks. Then it covers different communication standards for smart card–based applications and discusses the role of smart cards in various application areas as well as various open-source tools for the development and maintenance of smart card–based systems and applications. The final chapter explains the role of blockchain technology for securing smart card–based transactions and quantum cryptography for designing secure smart card–based algorithms. Smart Card Security: Applications, Attacks, and Countermeasures provides you with a broad overview of smart card technology and its various applications.

Smart Card. Research and Applications

For many, smart grids are the biggest technological revolutionsince the Internet. They have the potential to reduce carbondioxide emissions, increase the reliability of electricity supply,and increase the efficiency of our energy infrastructure. Smart Grid Applications, Communications, and Securityexplains how diverse technologies play hand-in-hand in building andmaintaining smart grids around the globe. The book delves into thecommunication aspects of smart grids, provides incredible insightinto power electronics, sensing, monitoring, and controltechnologies, and points out the potential for new technologies andmarkets. Extensively cross-

referenced, the book contains comprehensivecoverage in four major parts: Part I: Applications provides a detailedintroduction to smart grid applications—spanning thetransmission, distribution, and consumer side of the electricitygrid Part II: Communications discusses wireless,wireline, and optical communication solutions—from thephysical layers up to sensing, automation, and control protocolsrunning on the application layers Part III: Security deals with cybersecurity—sharpening the awareness of security threats,reviewing the ongoing standardization, and outlining the future ofauthentication and encryption key management Part IV: Case Studies and Field Trials presentsself-contained chapters of studies where the smart grid of tomorrowhas already been put into practice With contributions from majorindustry stakeholders such as Siemens, Cisco, ABB, and Motorola,this is the ideal book for both engineering professionals andstudents.

Smart Card Programming and Security

Smart cards are an established security research area with a very unique pr- erty: it integrates numerous sub?elds of IT Security, which often appear sc- tered and only loosely connected. Smart card research unites them by providing a common goal: advancing the state of the art of designing and deploying small tokens to increase the security in Information Technology. CARDIS has a tradition of more than one decade, and has established itself asthepremier conferencefor researchresultsinsmartcardtechnology.As smart card

research is unique, so is CARDIS; the conference successfully attracts a- demic and industrial researchers without compromising in either way. CARDIS accommodates applied research results as well as theoretical contributions that might or might not become practically relevant. The key to making such a m- ture attractive to both academia and industry is simple: quality of contributions and relevance to the overall subject. This year's CARDIS made it easy to continue this tradition: we received 76 papers, nearly all of them relevant to the focus of CARDIS and presenting high-quality researchresults. The ProgramCommittee workedhard on selecting the best 25 papers to be presented at the conference. We are very grateful to the members of the Program Committee and the additional referees for generously spending their time on the di?cult task of assessing the value of submitted papers. Daniel Schreckling provided invaluable assistance in handling submissions, managing review reports and editing the proceedings. The assistance of Jordi Castell` a in handling practical aspects of the conference preparation is also greatly appreciated.

Emerging Security Algorithms and Techniques

Since1994,CARDIShasbeentheforemostinternationalconferencededicatedto smart card research and applications. Every two years, the scienti?c community congregates to present new ideas and discuss recent developments with both an academicandindustrialfocus.Followingtheincreasedcapabilitiesofs

martcards anddevices,CARDIS has becomea majoreventfor the discussionofthe various issuesrelat edtotheuseofsmallelectronictokensintheprocessofhum an-machine interactions.Thescopeoftheconferenceincl udesnumeroussub?eldssuchasn- working,e?cientimple mentations,physicalsecurity,biometrics,andso on. This year's CARDIS was held in London, UK, on September 8–11, 2008. It was organized by the Smart Card Centre, Information Security Group of the Royal Holloway, University of London. Thepresentvolumecon tainsthe21papersthatwereselectedfromthe51s-missions to the conference. The 22 members of the program committee worked hard in order to evaluate each submission with at least three reviews and agree on a high quality ?nal program. Additionally, 61 external reviewers helped the committee with their expertise. Two invited talks completed the technical p- gram. The ?rst one, given by Ram Banerjee and Anki Nelaturu, was entitled "Getting Started with Java Card 3.0 Platform". The second one, given by Aline Gouget, was about "Recent Advances in Electronic Cash Design" and was c- pleted by an abstract provided in these proceedings.

Security and Privacy in the Age of Ubiquitous Computing

As magnetic stripe cards are being replaced by chip cards that offer consumers and business greater protection against fraud, a new standard for this technology is being introduced by Europay, MasterCard and Visa (EMV). This volume presents a comprehensive overview of the EMV chip solution and

explains how this technology provides a chip migration path, where interoperability plays a central role in the business model. The work offers an understanding of the security problems associated with magnetic stripe cards, and presents the business case for chip migration. Moreover, it explains the implementation of multi-application selection mechanisms in EMV chip cards and terminals, and shows you how to design a multi-application EMV chip card layout.

Smart Card Research and Advanced Applications

This volume constitutes the thoroughly refereed post-proceedings of the Third International Conference on Smart Card Research and Advanced Applications, CARDIS'98, held in Louvain-la-Neuve, Belgium in September 1998. The 35 revised full papers presented were carefully reviewed and updated for inclusion in this book. All current aspects of smart card research and applications development are addressed, in particular: Java cards, electronic commerce, efficiency, security (including cryptographic algorithms, cryptographic protocols, and authentication), and architecture.

Recent Trends in Network Security and Applications

This is the third revised edition of the established and trusted RFID Handbook; the most comprehensive introduction to radio frequency identification (RFID)

available. This essential new edition contains information on electronic product code (EPC) and the EPC global network, and explains near-field communication (NFC) in depth. It includes revisions on chapters devoted to the physical principles of RFID systems and microprocessors, and supplies up-to-date details on relevant standards and regulations. Taking into account critical modern concerns, this handbook provides the latest information on: the use of RFID in ticketing and electronic passports; the security of RFID systems, explaining attacks on RFID systems and other security matters, such as transponder emulation and cloning, defence using cryptographic methods, and electronic article surveillance; frequency ranges and radio licensing regulations. The text explores schematic circuits of simple transponders and readers, and includes new material on active and passive transponders, ISO/IEC 18000 family, ISO/IEC 15691 and 15692. It also describes the technical limits of RFID systems. A unique resource offering a complete overview of the large and varied world of RFID, Klaus Finkenzeller's volume is useful for end-users of the technology as well as practitioners in auto ID and IT designers of RFID products. Computer and electronics engineers in security system development, microchip designers, and materials handling specialists benefit from this book, as do automation, industrial and transport engineers. Clear and thorough explanations also make this an excellent introduction to the topic for graduate level students in electronics and industrial engineering design. Klaus Finkenzeller was awarded the Fraunhofer-Smart Card Prize 2008 for the second edition of this publication, which was celebrated for

being an outstanding contribution to the smart card field.

RFID and Contactless Smart Card Applications

Smart cards or IC cards offer a huge potential for information processing purposes. The portability and processing power of IC cards allow for highly secure conditional access and reliable distributed information processing. IC cards that can perform highly sophisticated cryptographic computations are already available. Their application in the financial services and telecom industries are well known. But the potential of IC cards go well beyond that. Their applicability in mainstream Information Technology and the Networked Economy is limited mainly by our imagination; the information processing power that can be gained by using IC cards remains as yet mostly untapped and is not well understood. Here lies a vast uncovered research area which we are only beginning to assess, and which will have a great impact on the eventual success of the technology. The research challenges range from electrical engineering on the hardware side to tailor-made cryptographic applications on the software side, and their synergies. This volume comprises the proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000), which was sponsored by the International Federation for Information Processing (IFIP) and held at the Hewlett-Packard Labs in the United Kingdom in September 2000. CARDIS

conferences are unique in that they bring together researchers who are active in all aspects of design of IC cards and related devices and environments, thus stimulating synergy between different research communities from both academia and industry. This volume presents the latest advances in smart card research and applications, and will be essential reading for smart card developers, smart card application developers, and computer science researchers involved in computer architecture, computer security, and cryptography.

Smart Grid Applications, Communications, and Security

Multi-application smart cards have yet to realise their enormous potential, partly because few people understand the technology, market, and behavioural issues involved. Here, Mike Hendry sets out to fill this knowledge gap with a comprehensive and accessible guide. Following a review of the state-of-the-art in smart card technology, the book describes the business requirements of each smart-card-using sector, and the systems required to support multiple applications. Implementation aspects, including security, are treated in detail and numerous international case studies cover identity, telecoms, banking and transportation applications. Lessons are drawn from these studies to help deliver more successful projects in the future. Invaluable for users and integrators specifying, evaluating and integrating multi-application systems, the book will also be useful to terminal, card and system designers; network, IT

and security managers; and software specialists.

Internet of Things Security

Even in the age of ubiquitous computing, the importance of the Internet will not change and we still need to solve conventional security issues. In addition, we need to deal with new issues such as security in the P2P environment, privacy issues in the use of smart cards, and RFID systems. Security and Privacy in the Age of Ubiquitous Computing addresses these issues and more by exploring a wide scope of topics. The volume presents a selection of papers from the proceedings of the 20th IFIP International Information Security Conference held from May 30 to June 1, 2005 in Chiba, Japan. Topics covered include cryptography applications, authentication, privacy and anonymity, DRM and content security, computer forensics, Internet and web security, security in sensor networks, intrusion detection, commercial and industrial security, authorization and access control, information warfare and critical protection infrastructure. These papers represent the most current research in information security, including research funded in part by DARPA and the National Science Foundation.

Smart Cards

Intended for Java Card applet developers, platform implementers, and technical managers seeking an overall understanding of Java Card technology, this guide provides an introduction to the development of

applications with Java Card technology based on Java Card version 2.1. Includes an introduction to the platform, an overview and discussion of the technology, a programming guide, and tips. Annotation copyrighted by Book News, Inc., Portland, OR

Social and Human Elements of Information Security: Emerging Trends and Countermeasures

With Smart Card Programming the reader will have the expert guidance he need to work with smart cards. The book offers a comprehensive guide, to the technological aspects related to smart cards, providing an high level overview of the technological panorama and giving an in-depth technical coverage about the related architectures, programming paradigms and APIs. The first part of the book introduces the smart card technologies, the general concepts and a few case studies. It is addressed also to non-technical reader who wishes an high level overview on smart card world. The second part of the book is a technical guide to smart card specifications and programming paradigms. It dives into technical topics about smart card programming and applications development in C/C++, C#, Visual Basic and Java. Key features include: - Contact and Contactless Cards - ISO 7816 - NFC - JavaCard Framework - PC/SC - PKCS#11 - OpenCard Framework - Java - Smart Card I/O - GlobalPlatform - EMV

Smart Card Handbook

This extensively updated edition of the popular book offers a current overview of the ways smart cards address the computer security issues of today's varied applications. Brand-new discussions on multiapplication operating systems, computer networks, and the Internet are included to keep technical and business professionals abreast of the latest developments in this field.

Smart Card Research and Advanced Applications

This book constitutes the refereed proceedings of the Second International Conference on Research in Smart Cards, E-smart 2001, held in Cannes, France, in September 2001. The 20 revised full papers presented were carefully reviewed and selected from 38 submissions. Among the topics addressed are biometrics, cryptography and electronic signatures on smart card security, formal methods for smart card evaluation and certification, architectures for multi-applications and secure open platforms, and middleware for smart cards and novel applications of smart cards.

Smart Card Security

New generations of IT users are increasingly abstracted from the underlying devices and platforms that provide and safeguard their services. As a result they may have little awareness that they are critically dependent on the embedded security devices that are becoming pervasive in daily modern life. Secure

Smart Embedded Devices, Platforms and Applications provides a broad overview of the many security and practical issues of embedded devices, tokens, and their operation systems, platforms and main applications. It also addresses a diverse range of industry/government initiatives and considerations, while focusing strongly on technical and practical security issues. The benefits and pitfalls of developing and deploying applications that rely on embedded systems and their security functionality are presented. A sufficient level of technical detail to support embedded systems is provided throughout the text, although the book is quite readable for those seeking awareness through an initial overview of the topics. This edited volume benefits from the contributions of industry and academic experts and helps provide a cross-discipline overview of the security and practical issues for embedded systems, tokens, and platforms. It is an ideal complement to the earlier work, Smart Cards Tokens, Security and Applications from the same editors.

Multi-application Smart Cards

Smart cards play an increasingly important role in everyday life. We encounter them as credit cards, loyalty cards, electronic purses, health cards, ands as secure tokens for authentication or digital signatures. Their small size and the compatibility of their form with the magnetic stripe card make them ideal carriers of personal information such as secret keys, passwords, customization profiles, and medical emergency information. This book provides a guide

for the rapid development of smart card applications using Java and the OpenCard Framework. It gives you the basic information you need about smart cards and how they work. A smart card provided with the book will help you to obtain first-hand experience.

Smart Card

Smart cards are playing an increasingly important role in areas such as ban- 1 king,electroniccommerce,andtelecommunications. TheJavaCard language hasbeenproposedasahigh-levellanguageforprogrammingmulti-application smartcards. Theuseofahigh-levellanguagecanfacilitatethedevelopmentand veri'cation of software for smart cards. The modest code size and the imp- tanceoftheapplicationareasimp liesthatitisbothpossibleanddesirableto developandappl yformalmethodsintheconstructionofsafeandsecureJava Cardsoftware. Thepresentvolumeconstitutestheprocee dingsoftheJavaCardworkshop heldinCannes,14September2000. TheworkshopgrewoutoftheINRIAAction deRechercheCoop ´erative"JavaCard"andwasorganizedincollaborationwith the Java Card Forum. A call for papers resulted in 14 submissions of which theprogramcommitteeselected1 1papersforpresentationattheworkshop. In addition,the workshopfeaturedaninvitedtalkbyDanielLeM ´etayer,Trusted Logic,onformalmethodsandsmartcardsecurity. WewishtothankCatherine Godest and Maryse Renaud for their help with preparing the proceedings for

thisworkshop. February2001IsabelleAttali
ThomasJensen 1 ItshouldbenotedthatJavaCardisatrade
markofSunMicrosystems. Organization
ProgramCommittee ProgramChair:
IsabelleAttali(INRIA,France)
ThomasJensen(IRISA/CNRS,France)
Committeemembers: ChristianGoire(BullCP8,France)
SebastianHans(SunMicrosystems,USA)
PieterHartel(UniversityofSouthampton,UK)
PeterHoneyman(UniversityofMichigan,USA)
PierreParadinas(Gemplus,France)
JoachimPosegga(SAPCorporateResearch,Germany)
TableofContents InvitedTalk

Formal Methods in Context: Security and
Java Card D. Bolignano, D. Le Métayer, and C.
Loiseaux Trusted Logic www. trusted-logic. fr 1.
Security and Java Card: An Ideal Application Area for
Formal Methods The benefits of formal methods for
software engineering have been described at length
in many research papers. They include among others:
Better understanding and improved communication
through unambiguous descriptions. Early bug
detection thanks to the formalisation of specifications.

Multi-application Smart Cards

Power analysis attacks allow the extraction of secret
information from smart cards. Smart cards are used in
many applications including banking, mobile

communications, pay TV, and electronic signatures. In all these applications, the security of the smart cards is of crucial importance. Power Analysis Attacks: Revealing the Secrets of Smart Cards is the first comprehensive treatment of power analysis attacks and countermeasures. Based on the principle that the only way to defend against power analysis attacks is to understand them, this book explains how power analysis attacks work. Using many examples, it discusses simple and differential power analysis as well as advanced techniques like template attacks. Furthermore, the authors provide an extensive discussion of countermeasures like shuffling, masking, and DPA-resistant logic styles. By analyzing the pros and cons of the different countermeasures, this volume allows practitioners to decide how to protect smart cards.

Java Card for E-Payment Applications

A practical guide to the specification, design, and programming of smart card systems for working applications. More than 3 billion smartcards are produced every year. Generally defined as any pocket-sized card with embedded integrated circuits or chips, they have a huge number of applications including travel cards, chip and pin cards, pet tags, mobile phone SIMs and pallet trackers. Now with modern Smart Card technology such as Java Card and Basic Card it is possible for everyone to create his or her own applications on a smart card. This book provides generic solutions for programming smart cards, enabling the creation of working applications and

systems. Key features: Presents a comprehensive introduction to the topic of smart cards, explaining component elements and the smart card microcontrollers. Sets out information on operating systems with case studies of a range of applications including credit card security, mobile phones and transport payment cards. Gives detailed advice on the monitoring of smart card applications, recognizing potential attacks on security and improving system integrity. Provides modules and examples so that all types of systems can be built up from a small number of individual components. Offers guidelines on avoiding and overcoming design errors. Ideal for practising engineers and designers looking to implement smart cards in their business, it is also a valuable reference for postgraduate students taking courses on embedded system and smart card design.

Smart Card Research and Advanced Applications

Cyber security is the protection of information systems, hardware, software, and information as well from theft, damages, interruption or misdirection to any of these resources. In other words, cyber security focuses on protecting computers, networks, programs and data (in use, in rest, in motion) from unauthorized or unintended access, change or destruction. Therefore, strengthening the security and resilience of cyberspace has become a vital homeland security mission. Cyber security attacks are growing exponentially. Security specialists must occupy in the lab, concocting new schemes to preserve the

resources and to control any new attacks. Therefore, there are various emerging algorithms and techniques viz. DES, AES, IDEA, WAKE, CAST5, Serpent Algorithm, Chaos-Based Cryptography McEliece, Niederreiter, NTRU, Goldreich–Goldwasser–Halevi, Identity Based Encryption, and Attribute Based Encryption. There are numerous applications of security algorithms like cyber security, web security, e-commerce, database security, smart card technology, mobile security, cloud security, digital signature, etc. The book offers comprehensive coverage of the most essential topics, including: Modular Arithmetic, Finite Fields Prime Number, DLP, Integer Factorization Problem Symmetric Cryptography Asymmetric Cryptography Post-Quantum Cryptography Identity Based Encryption Attribute Based Encryption Key Management Entity Authentication, Message Authentication Digital Signatures Hands-On "SageMath" This book serves as a textbook/reference book for UG, PG, PhD students, Teachers, Researchers and Engineers in the disciplines of Information Technology, Computer Science and Engineering, and Electronics and Communication Engineering.

Smart Cards, Tokens, Security and Applications

Building on previous editions, this third edition of the Smart Card Handbook offers a completely updated overview of the state of the art in smart card technology. Everything you need to know about smart cards and their applications is covered! Fully revised,

this handbook describes the advantages and disadvantages of smart cards when compared with other systems, such as optical cards and magnetic stripe cards and explains the basic technologies to the reader. This book also considers the actual status of appropriate European and international standards. Features include: New sections on: smart card applications (PKCS #15, USIM, Tachosmart). smart card terminals: M.U.S.C.L.E., OCF, MKT, PC/SC. contactless card data transmission with smart cards. Revised and updated chapters on: smart cards in the telecommunications industry (GSM, UMTS, (U)SIM application toolkit, decoding of the files of a GSM card). smart card security (new attacks, new protection methods against attacks). A detailed description of the physical and technical properties and the fundamental principles of information processing techniques. Explanations of the architecture of smart card operating systems, data transfer to and from the smart card, command set and implementation of the security mechanisms and the function of the smart card terminals. Current applications of the technology on mobile telephones, telephone cards, the electronic purse and credit cards. Discussions on future developments of smart cards: USB, MMU on microcontroller, system on card, flash memory and their usage. Practical guidance on the future applications of smart cards, including health insurance cards, e-ticketing, wireless security, digital signatures and advanced electronic payment methods. "The book is filled with information that students, enthusiasts, managers, experts, developers, researchers and programmers will find useful. The book is well structured and provides a good account

of smart card state-of-the-art technology... There is a lot of useful information in this book and as a practicing engineer I found it fascinating, and extremely useful." Review of second edition in Measurement and Control. 'The standard has got a lot higher, if you work with smart cards then buy it! Highly recommended.' Review of second edition in Journal of the Association of C and C++ Programmers. Visit the Smart Card Handbook online at www.wiley.co.uk/commstech/

RFID Handbook

Smart Cards

Since1994,CARDIShasbeentheforemostinternationalconferencededicatedto smart card research and applications. Every two years, the scienti?c community congregates to present new ideas and discuss recent developments with both an academica ndindustrialfocus.Followingtheincreasedcapabilitiesofsmartcards anddevices,CARDIS has becomea majoreventfor the discussionofthe various issuesrelat edtotheuseofsmallelectronictokensintheprocessofhuman-machine interactions.Thescopeoftheconferenceincl udesnumeroussub?eldssuchasn- working,e?cientimplementations,physicalsecurity,biometrics,andso on. This year's CARDIS was held in London, UK, on September 8–11, 2008. It was organized by the Smart Card Centre, Information Security Group of the Royal Holloway, University of London. Thepresentvolumecontainsthe21papersthatwereselectedfromthe51s-

missions to the conference. The 22 members of the program committee worked hard in order to evaluate each submission with at least three reviews and agree on a high quality ?nal program. Additionally, 61 external reviewers helped the committee with their expertise. Two invited talks completed the technical p- gram. The ?rst one, given by Ram Banerjee and Anki Nelaturu, was entitled "Getting Started with Java Card 3.0 Platform". The second one, given by Aline Gouget, was about "Recent Advances in Electronic Cash Design" and was c- pleted by an abstract provided in these proceedings.

Smart Card Programming

This book constitutes the thoroughly refereed post-conference proceedings of the 10th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications, CARDIS 2011, held in Leuven, Belgium, in September 2011. The 20 revised full papers presented were carefully reviewed and selected from 45 submissions. The papers are organized in topical sections on smart cards system security, invasive attacks, new algorithms and protocols, implementations and hardware security, non-invasive attacks, and Java card security.

Secure Smart Embedded Devices, Platforms and Applications

The Third International Conference on Network Security and Applications (CNSA-2010) focused on all technical and practical aspects of security and its

applications for wired and wireless networks. The goal of this conference is to bring together researchers and practitioners from academia and industry to focus on understanding modern security threats and countermeasures, and establishing new collaborations in these areas. Authors are invited to contribute to the conference by submitting articles that illustrate research results, projects, survey work and industrial experiences describing significant advances in the areas of security and its applications, including: • Network and Wireless Network Security • Mobile, Ad Hoc and Sensor Network Security • Peer-to-Peer Network Security • Database and System Security • Intrusion Detection and Prevention • Internet Security, and Applications Security and Network Management • E-mail Security, Spam, Phishing, E-mail Fraud • Virus, Worms, Trojon Protection • Security Threats and Countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc.) • Ubiquitous Computing Security • Web 2. 0 Security • Cryptographic Protocols • Performance Evaluations of Protocols and Security Application There were 182 submissions to the conference and the Program Committee selected 63 papers for publication. The book is organized as a collection of papers from the First International Workshop on Trust Management in P2P Systems (IWTMP2PS 2010), the First International Workshop on Database Management Systems (DMS-2010), and the First International Workshop on Mobile, Wireless and Networks Security (MWNS-2010).

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION