Smart Card Programming And Security International Conference On Research In Smart Cards E Smart 200

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.

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.Followingtheincreasedcapabilitiesofsmartcards anddevices,CARDIS has becomea majoreventfor the discussionofthe various issuesrelatedtotheuseofsmallelectronictokensintheprocessofhuman-machine interactions.Thescopeoftheconferenceincludesnumeroussub?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.

As the field of information technology continues to grow and expand, it impacts more and more organizations worldwide. The leaders within these organizations are challenged on a continuous basis to develop and implement programs that successfully apply information technology applications. This is a collection of unique perspectives on the issues surrounding IT in organizations and the ways in which these issues are addressed. This valuable book is a compilation of the latest research in the area of IT utilization and management.

With the rapid technological development of information technology, computer systems and especially embedded systems are becoming more mobile and ub- uitous. Ensuring the security of these complex and yet resource-constraineds- temshasemergedasoneofthemostpressingchallengesforresearchers.Although there are a number of information security conferences that look at particular aspects of the challenge, we decided to create the Workshop in Information - curity Theory and Practices (WISTP) to consider the problem as a whole. In additiontheworkshopaimsto bringtogetherresearchersandpractitionersin- lated disciplines and encourage interchange and practical co-operation between academia and industry. Although this is the ?rst ever WISTP event, the response from researchers wassuperbwithover68paperssubmittedforpotentialinclusionintheworkshop and proceedings. The submissions were reviewed by at least three reviewers, in most cases by four, and for program committee (PC) papers at least ?ve reviewers. This long and rigorous process was only possible thanks to the hard work of the PC members and additional reviewers, listed in the following pages. We would like to express our gratitude to the PC members, who were very supportive from the very beginning of this project. Thanks are also due to the additional expert reviewers who helped the PC to select the ?nal 20 workshop papers for publication in the proceedings. Of course we highly appreciate the e?orts of all the authors who submitted papers to WISTP 2007. We hope they will contribute again to a future edition and encourage others to do so.

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.

Ad hoc and sensor networks are making their way from research to real-world deployments. Body and personal-area networks, intelligent homes, environmental monitoring or inter-vehicle communications: there is almost nothing left that is not going to be smart and networked. While a great amount of research has been devoted to the pure networking aspects, ad hoc and sensor networks will not be successfully deployed if security, dependability, and privacy issues are not addressed adequately. As the first book devoted to the topic, this volume constitutes the thoroughly refereed post-proceedings of the First European Workshop on Security in Ad-hoc and Sensor Networks, ESAS, 2004, held in Heidelberg, Germany in August 2004. The 17 revised full papers were carefully reviewed and selected from 55 submissions. Among the key topics addressed are key distribution and management, authentication, energy-aware cryptographic primitives, anonymity and pseudonymity, secure diffusion, secure peer-to-peer overlays, and RFIDs.

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.

The Proceedings of the International Conference on Information Engineering, Management and Security 2014 which happened at Christu Jyoti Institute of Technology.

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/

As a working tool for professionals, this easy-to-understand resource provides clear, detailed guidance on smart, credit and debit cards, JavCard and OpenCard Framework.

In today's world, smart cards play an increasingly important role in everyday life. We encounter them as credit cards, loyalty cards, electronic purses, health cards, and as secure tokens for authentication or digital signature. Their small size and the compatibility of their form with the magnetic stripe card make them the 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. It shows in detail how to develop applications that use smart cards by guiding you through examples step by step. A smart card provides you with the book will help you to quickly get some first hands-on experience. Das Buch bietet erstmals einen Leitfaden zur Entwicklung von Smartcard-Anwendungen mit Java (JDK ab Version 1.1.6) und OCF 1.1.1 auf dem Computer, sowie zur Entwicklung von Java Applets, die direkt auf einer Karte (Java Card) ausgeführt werden. Der erste Teil führt konzise in Grundlagen, Technologie und Anwendungsmöglichkeiten von Smartcard ein. Im zweiten Teil werden Ziel, Konzept, Architektur und Komponenten des OpenCard Framework detailliert beschrieben. Der dritte Teil demonstriert anhand einfacher Beispiele Aufbau und Design komplexer Anwendungen für den Karten- und den Host-Teil. Mit der beiliegenden Multi Function Card lassen sich die beschriebenen Beispiele leicht ausführen und weiterentwickeln.

This book constitutes the thoroughly refereed post-conference proceedings of the 8th International Conference on Security for Information Technology and Communications, SECITC 2015, held in Bucharest, Romania, in June 2015. The 17 revised full papers were carefully reviewed and selected from 36 submissions. In addition with 5 invited talks the papers cover topics such as Cryptographic Algorithms and Protocols, Security Technologies for IT&C, Information Security Management, Cyber Defense, and Digital Forensics.

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.

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.

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

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.

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-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.

This book provides the foundations for understanding hardware security and trust, which have become major concerns for national security over the past decade. Coverage includes security and trust issues in all types of electronic devices and systems such as ASICs, COTS, FPGAs, microprocessors/DSPs, and embedded systems. This serves as an invaluable reference to the state-of-the-art research that is of critical significance to the security of, and trust in, modern society's microelectronic-supported infrastructures.

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

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 ProgrammingLulu.com

The explosive demand for mobile communications is driving the development of wireless technology at an unprecedented pace. Unfortunately, this exceptional growth is also giving rise to a myriad of security issues at all levels from subscriber to network operator to service provider. Providing technicians and designers with a critical and comprehens

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.

The system over secure networks, but they contain sensitive data related to both the card holder and the system, that has to be kept private and confidential. The aim of the research is to conduct a risk management programme on the smart cards systems that are employed in e-business systems, suggest the best safeguards to be applied to better secure the smart card systems depending on the services and applications the smart card serves, and produce a simulation tool using a high level of abstraction programming language to be able to test the robustness of the proposed solutions. The study contributions are producing a Risk Analysis Guide specifically on smart card systems to support managerial decision making, modelling the current and proposed smart card systems including modelling the possible attacks using the Unified Modelling Language (UML) diagrams, and developing an executable model using SystemC and Transaction Level Modelling (TLM)extensions, which is a new way of modelling and testing smart card systems security. The security objectives have to be considered during the early stages of systems development and design; an executable model will give the designer the advantage of identifying vulnerabilities at an early stage, and therefore enhance the system security. The developed model is used to examine the effectiveness of number of authentication mechanisms with different probabilities of failure. Numbers of probable attacks on the current security protocol are modeled to identify vulnerabilities. The executable model shows that the smart card system security protocols and transactions need further improvement to withstand different types of security attacks.

Advances in Information Technology Research and Application: 2013 Edition is a ScholarlyBrief™ that delivers timely, authoritative, comprehensive, and specialized information about ZZZAdditional Research in a concise format. The editors have built Advances in Information Technology Research and Application: 2013 Edition on the vast information databases of ScholarlyNews.™ You can expect the information about Advances in Information Technology Research and Application: 2013 Edition in this book to be deeper than what you can access anywhere else, as well as consistently reliable, authoritative, informed, and relevant. The content of Advances in Information Technology Research and Application: 2013 Edition has been produced by the world's leading scientists, engineers, analysts, research institutions, and companies. All of the content is from peer-reviewed sources, and all of it is written, assembled, and edited by the editors at ScholarlyEditions™ and available exclusively from us. You now have a source you can cite with authority, confidence, and credibility. More information is available at http://www.ScholarlyEditions.com/.

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 systems 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.

Mary J. Cronin, a leading expert on using the Internet for business, provides an overview of the impact of the Internet on banking, and offers her vision of the future of electronic banking.

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.

The 5th International Workshop on Information Security Applications (WISA 2004) was held in Jeju Island, Korea during August 23-25, 2004. The workshop was sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI) and the Ministry of Information and Communication (MIC). The aim of the workshop is to serve as a forum for new conceptual and - perimental research results in the area of information security applications from the academic community as well as from the industry. The workshop program covers a wide range of security aspects including cryptography, cryptanalysis, network/system security and implementation aspects. The programcommittee received169 papersfrom 22 countries,andaccepted 37 papers for a full presentation track and 30 papers for a short presentation track. Each paper was carefully evaluated through peer-review by at least three members of the programcommittee. This volume contains revised versions of 36 papers accepted and presented in the full presentation track. Short papers were only published in the WISA 2004 pre-proceedings as preliminary versions and are allowed to be published elsewhere as extended versions. In addition to the contributed papers, Professors Gene Tsudik and Ross Andersongaveinvitedtalks,entitledSecurityinOutsourcedDatabasesandWhat does 'Security' mean for Ubiquitous Applications?, respectively.

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.

This book constitutes the thoroughly refereed post-proceedings of the First International Java Card Workshop held in Cannes, France, in September 2000. The 11 revised full papers presented were carefully reviewed and selected for inclusion in the book together with one invited paper. All current theoretical and application-oriented aspects of smart card security based on Java Card language programs are addressed.

A state-of-the-art guide to middleware technologies, and their pivotal role in communications networks. Middleware is about integration and interoperability of applications and services running on heterogeneous computing and communications devices. The services it provides - including identification, authentication, authorization, soft-switching, certification and security - are used in a vast range of global appliances and systems, from smart cards and wireless devices to mobile services and e-Commerce. Qusay H. Mahmoud has created an invaluable reference tool that explores the origins and current uses of middleware (highlighting the importance of such technologies as CORBA, J2EE and JMS) and has thus compiled the roadmap to future research in this area. Middleware for Communications: discusses the emerging fields of Peer-to-Peer (P2P) and grid middleware detailing middleware platforms such as JXTA and the Globus middleware toolkit. shows how Middleware will play a significant role in mobile computing. presents a Platform Supporting Mobile Applications (PLASMA) - a middleware platform that consists of components for location, event, and profile handling of Location-Based Services. introduces middleware security focusing on the appropriate aspects of CORBA, J2EE, and .NET and demonstrates how to realize complex security capabilities such as role-based access control (RBAC) and mandatory access control (MAC). discusses how Quality of Service (QoS) component middleware can be combined with Model Driven Architecture (MDA) technologies to rapidly develop, generate, assemble and deploy flexible communications applications. This incomparable overview of middleware for communications is suitable for graduate students and researchers in communications and computing departments. It is also an authoritative guide for engineers and developers working on distributed systems, mobile computing and networked appliances.

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

This volume provides the academic and industrial community with a medium for presenting original research and applications related to information assurance and security using computational intelligence techniques. It details current research on information assurance and security regarding both the theoretical and methodological aspects, as well as various applications in solving real world problems using computational intelligence.

"This book provides coverage of recent advances in the area of secure software engineering that address the various stages of the development process from requirements to design to testing to implementation"--Provided by publisher.

This book constitutes the refereed proceedings of the Second International Conference on Security in Pervasive Computing, SPC 2005, held in Boppard, Germany in April 2005. The 14 revised full papers and 3 revised short papers presented together with abstracts of 5 invited talks were carefully reviewed and selected from 48 submissions. The papers are organized in topical sections on smart devices and applications, authentication, privacy and anonymity, and access control and information flow.

This book constitutes the refereed proceedings of the 12th European Symposium on Programming, ESOP 2003, held in Warsaw, Poland, in April 2003. The 25 revised full papers presented together with two invited papers were carefully reviewed and selected from 99 submissions. Among the topics addressed are programming paradigms and their integration, program semantics, calculi of computation, security, advanced type systems, program analysis, program transformation, and practical algorithms based on theoretical developments.

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.

A unique overview of network security issues, solutions, and methodologies at an architectural and research level Network Security provides the latest research and addresses likely future developments in network security protocols, architectures, policy, and implementations. It covers a wide range of topics dealing with network security, including secure routing, designing firewalls, mobile agent security, Bluetooth security, wireless sensor networks, securing digital content, and much more. Leading authorities in the field provide reliable information on the current state of security protocols, architectures, implementations, and policies. Contributors analyze research activities, proposals, trends, and state-of-the-art aspects of security and provide expert insights into the future of the industry. Complete with strategies for implementing security mechanisms and techniques, Network Security features: * State-of-the-art technologies not covered in other books, such as Denial of Service (DoS) and Distributed Denial-of-Service (DDoS) attacks and countermeasures * Problems and solutions for a wide range of network technologies, from fixed point to mobile * Methodologies for real-time and non-real-time applications and protocols