Understanding Pki Concepts Standards And Deployment Considerations Kaleidoscope

Security and privacy are paramount concerns in information processing systems, which are vital to business, government and military operations and, indeed, society itself. Meanwhile, the expansion of the Internet and its convergence with telecommunication networks are providing incredible connectivity, myriad applications and, of course, new threats. Data and Applications Security XVII: Status and Prospects describes original research results, practical experiences and innovative ideas, all focused on maintaining security and privacy in information processing systems and applications that pervade cyberspace. The areas of coverage include: -Information Warfare, -Information Assurance, -Security and Privacy, -Authorization and Access Control in Distributed Systems, -Security Technologies for the Internet, -Access Control Models and Technologies, -Digital Forensics. This book is the seventeenth volume in the series produced by the International Federation for Information Processing (IFIP) Working Group 11.3 on Data and Applications Security. It presents a selection of twenty-six updated and edited papers from the Seventeenth Annual IFIP TC11 / WG11.3 Working Conference on Data and Applications Security held at Estes Park, Colorado, USA in August 2003, together with a report on the conference keynote speech and a summary of the conference panel. The contents demonstrate the richness and vitality of the discipline, and other directions for future research in data and applications security. Data and Applications Security XVII: Status and Prospects is an invaluable resource for information assurance researchers, faculty members and graduate students, as well as for individuals engaged in research and development in the information technology sector.

This book constitutes the refereed proceedings of the 26th International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2007. The 33 revised full papers and 16 short papers are organized in topical sections on safety cases, impact of security on safety, fault tree analysis, safety analysis, security aspects, verification and validation, platform reliability, reliability evaluation, formal methods, static code analysis, safety-related architectures.

Cryptography is now ubiquitous – moving beyond the traditional environments, such as government communications and banking systems, we see cryptographic techniques realized in Web browsers, e-mail programs, cell phones, manufacturing systems, embedded software, smart buildings, cars, and even medical implants. Today's designers need a comprehensive understanding of applied cryptography. After an introduction to cryptography and data security, the authors explain the main techniques in modern cryptography, with chapters addressing stream ciphers, the Data Encryption Standard (DES) and 3DES, the Advanced Encryption Standard (AES), block ciphers, the RSA cryptosystem, public-key cryptosystems based on the discrete logarithm problem, elliptic-curve cryptography (ECC), digital signatures, hash functions, Message Authentication Codes (MACs), and methods for key establishment, including certificates and public-key infrastructure (PKI). Throughout the book, the authors focus on communicating the essentials and keeping the mathematics to a minimum, and they move quickly from explaining the foundations to describing practical implementations, including recent topics such as lightweight ciphers for RFIDs and mobile devices, and current key-

length recommendations. The authors have considerable experience teaching applied cryptography to engineering and computer science students and to professionals, and they make extensive use of examples, problems, and chapter reviews, while the book's website offers slides, projects and links to further resources. This is a suitable textbook for graduate and advanced undergraduate courses and also for self-study by engineers.

This book constitutes the proceedings of the 23rd International Conference on Discovery Science, DS 2020, which took place during October 19-21, 2020. The conference was planned to take place in Thessaloniki, Greece, but had to change to an online format due to the COVID-19 pandemic. The 26 full and 19 short papers presented in this volume were carefully reviewed and selected from 76 submissions. The contributions were organized in topical sections named: classification; clustering; data and knowledge representation; data streams; distributed processing; ensembles; explainable and interpretable machine learning; graph and network mining; multi-target models; neural networks and deep learning; and spatial, temporal and spatiotemporal data.

Frameworks for ICT Policy: Government, Social and Legal Issues is a reference on ICT policy framework and a guide to those who are involved in ICT policy formulation, implementation, adoption, monitoring, evaluation and application. This comprehensive publication provides background information for scholars and researchers who are interested in carrying out research on ICT policies and promotes the understanding of policies guiding technology.

Summary: Chapters in "Critical Insights From A Practitioner Mindset" have been grouped into four categories: (1) the New digital economy; (2) e-government practices; (3) identity and access management; and (4) identity systems implementation. These areas are considered to be crucial subsets that will shape the upcoming future and influence successful governance models. "Critical Insights From A Practitioner Mindset" is eminently readable and covers management practices in the government field and the efforts of the Gulf Cooperation Council (GCC) countries and the United Arab Emirates government. The book is key reading for both practitioners and decision-making authorities. Key Features: Is highly practical and easy to read. Comprehensive, detailed and through theoretical and practical analysis. Covers issues, and sources rarely accessed, on books on this topic. The Author: Dr Al-Khouri is the Director General (Under Secretary) of the Emirates Identity Authority: a federal government organisation established in 2004 to rollout and manage the national identity management infrastructure program in the United Arab Emirates. He has been involved in the UAE national identity card program since its early conceptual phases during his work with the Ministry of Interior. He has also been involved in many other strategic government initiatives in the past 22 years of his experience in the government sector. Contents: The new digital economy: Emerging markets and digital economy: building trust in the virtual world Biometrics technology and the new economy: a review of the field and the case of the United Arab Emirates E-government practices: PKI in government digital identity management systems An innovative approach for e-government transformation PKI in government identity management systems PKI technology: a government experience The role of digital certificates in contemporary government systems Identity and access management: Optimizing identity and access management (IAM) frameworks Towards federated identity management across GCC: a solution's framework Contemporary identity systems

implementation: Re-thinking enrolment in identity schemes Targeting results: lessons learned from UAE National ID Program"
"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.
As computers are increasingly embedded, ubiquitous and wirelessly connected, security becomes imperative; this has led to the development of the notion of a 'trusted platform', the chief characteristic of which is the possession of a trusted hardware element which is able to check all or part of the software running on this platform. This enables parties to verify the software environment running on a remote trusted platform, and hence to have some trust that the data sent to that machine will be processed in accordance with agreed rules. This new text introduces recent technological developments, and surveys current approaches to providing trusted platforms. It also includes application examples. The core of the book is based on an open workshop on Trusted Computing, held at Royal Holloway, University of London, UK.
This book constitutes the refereed proceedings of the Second International Conference on Mobile Ad-hoc and Sensor Networks, MSN 2006, held in Hong Kong, China in December 2006. The 73 revised full papers address all current issues in mobile ad hoc and sensor networks and are organized in topical sections on routing, network protocols, security, energy efficiency, data processing, and deployment.
These proceedings contain the papers selected for presentation at the 23rd Inter- tional Information Security Conference (SEC 2008), co-located with IFIP World Computer Congress (WCC 2008), September 8–10, 2008 in Milan, Italy. In - sponse to the call for papers, 143 papers were submitted to the conference. All - pers were evaluated on the basis of their signi?cance, novelty,and technical quality, and reviewed by at least three members of the program committee. Reviewing was blind meaning that the authors were not told which committee members reviewed which papers. The program committee meeting was held electronically, holding - tensive discussion over a period of three weeks. Of the papers submitted, 42 full papers and 11 short papers were selected for presentation at the conference. A conference like this just does not happen; it depends on the volunteer efforts of a host of individuals. There is a long list of people who volunteered their time and energy to put together the conference and who deserve acknowledgment. We thank all members of the program committee and the external reviewers for their hard work in the paper evaluation. Due to the large number of submissions, p- gram committee members were required to complete their reviews in a short time frame. We are especially thankful to them for the commitment they showed with their active participation in the electronic discussion.
This book constitutes the refereed proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2003, held in Taipei, Taiwan in November/December 2003. The 32 revised full papers presented together with one invited paper were carefully reviewed and selected from 188 submissions. The papers are organized

in topical sections on public key cryptography, number theory, efficient implementations, key management and protocols, hash functions, group signatures, block cyphers, broadcast and multicast, foundations and complexity theory, and digital signatures.
Annotation. Continuing the tradition of Journal of Management Information Systems, this strictly refereed series of research volumes offers an unparalleled lasting record of the field of Information Systems. Featuring brand new material specifically written for this series, each volume presents both knowledge aboutorganizational systems, and methods for creating new knowledge in the discipline. To further the field¿s continuing development, the series is designed to serve researchers as well as practitioners. AMIS publishes several topical volumes each year, edited by leading authorities in the various subfields of IS.
It's your job to make email safe. Where do you start? In today's national and global enterprises where business is conducted across time zones and continents, the "e" in email could stand for "essential." Even more critical is rock-solid email security. If you're the person charged with implementing that email security strategy, this book is for you. Backed with case studies, it offers the nuts-and-bolts information you need to understand your options, select products that meet your needs, and lock down your company's electronic communication systems. Review how email operates and where vulnerabilities lie Learn the basics of cryptography and how to use it against invaders Understand PKI (public key infrastructure), who should be trusted to perform specific tasks, how PKI architecture works, and how certificates function Identify ways to protect your passwords, message headers, and commands, as well as the content of your email messages Look at the different types of devices (or "tokens") that can be used to store and protect private keys
This book constitutes the proceedings of the 9th Workshop on RFID Security and Privacy, RFIDsec 2013, held in Graz, Austria, in July 2013. The 11 papers presented in this volume were carefully reviewed and selected from 23 submissions. RFIDsec deals with topics of importance to improving the security and privacy of RFID, NFC, contactless technologies, and the Internet of Things. RFIDsec bridges the gap between cryptographic researchers and RFID developers.
PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIESSeries meets all standards put forth by CNSS 4011 & 4013A!Access control protects resources against unauthorized viewing, tampering, or destruction. They serve as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. Revised and updated with the latest data from this fast paced field, Access Control, Authentication, and Public Key Infrastructure defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs. It looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them. It provides a student and professional resource that details how to put access control systems to work as well as testing and managing them. New to the Second Edition: Updated references to Windows 8 and Outlook 2011 A new discussion of recent Chinese hacking incidence Examples depicting the risks associated with a missing unencrypted laptop containing private data. New sections on the Communications Assistance for Law Enforcement Act (CALEA) and granting Windows folder permissions are added. New information on the Identity Theft Enforcement and Restitution Act and

the Digital Millennium Copyright Act (DMCA).

Access Control, Authentication, and Public Key Infrastructure provides a unique, in-depth look at how access controls protect resouces against unauthorized viewing, tampering, or destruction and serves as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. Written by industry experts, this book defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs, before looking at the risks, threats, and vulerabilities prevalent in information systems and IT infrastructures and ways of handling them. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully put access control systems to work as well as test and manage them. The Jones & Bartlett Learning: Information Systems Security & Assurance Series delivers fundamental IT Security principles packed with real-world applications and examples for IT Security, Cybersecurity, Information Assurance, and Information Systems Security programs, Authored by Certified Information Systems Security Professionals (CISSPs), and reviewed by leading technical experts in the field, these books are current, forward-thinking resources that enable readers to solve the cybersecurity challenges of today and tomorrow.

"This book compiles estimable research on the global trend toward the rapidly increasing use of information technology in the public sector, discussing such issues as e-government and e-commerce; project management and information technology evaluation; system design and data processing; security and protection; and privacy, access, and ethics of public information technology"--Provided by publisher.

The third successful completion of the INDOCRYPT conference series marks the acceptance of the series by the international research community as a forum for presenting high-quality research.It also marks the coming of age of cryptology research in India. The authors for the submitted papers were spread across 21 countries and 4 continents, which goes a long way to demonstrate the international interest and visibility of INDOCRYPT.In the previous two conferences, the submissions from India originated from only two institutes; this increased to six for the 2002 conference.Thus INDOCRYPT is well set on the path to achieving two main ob jectives – to provide an international platform for presenting high-quality research and to stimulate cryptology research in India. The opportunity to serve as a program co-chair for the third INDOCRYPT carries a special satisfaction for the second editor.Way back in 1998, the sci- ti?c analysis group of DRDO organized a National Seminar on Cryptology and abbreviated it as NSCR.On attending the seminar, the second editor suggested that the conference name be changed to INDOCRYPT.It is nice to see that this suggestion was taken up, giving us the annual INDOCRYPT conference - ries.Of course, the form, character, and execution of the conference series was the combined e?ort of the entire Indian cryptographic community under the dynamic leadership of Bimal Roy.

This book constitutes the refereed proceedings of the 5th European Public Key Infrastructure Workshop: Theory and Practice, EuroPKI 2008, held in Trondheim, Norway, in June 2008. The 15 revised full papers presented together with 1 invited paper were carefully reviewed and selected from 37 submissions. Ranging from theoretical and foundational topics to applications and

regulatory issues in various contexts, the papers focus on all research and practice aspects of PKI and show ways how to construct effective, practical, secure and low cost means for assuring authenticity and validity of public keys used in large-scale networked services.

This is a book of fresh insights, perspectives, strategies, and approaches for managing electronic records and archives. The authors draw on first-hand experience to present practical solutions, including recommendations for building and sustaining strong electronic records programs.

Introduces the concepts of public key infrastructure design and policy and discusses use of the technology for computer network security in the business environment.

Thisbookcontainsthepostproceedingsofthe6thEuropeanWorkshoponPublic Key Services, Applications and Infrastructures, which was held at the CNR Research Area in Pisa, Italy, in September 2009. The EuroPKI workshop series focuses on all research and practice aspects of public key infrastructures, services and applications, and welcomes original research papers and excellent survey contributions from academia, government, and industry. Previous events of the series were held in: Samos, Greece (2004); Kent, UK (2005); Turin, Italy, (2006); Palma de Mallorca, Spain, (2007); and Trondheim, Norway (2008). From the original focus on public key infrastructures, EuroPKI interests - panded to include advanced cryptographic techniques, applications and (more generally) services. The Workshops brings together researchersfrom the cryp- graphiccommunity as well as fromthe applied security community, as witnessed by the interesting program. Indeed, this volume holds 18 refereed papers and the presentation paper by the invited speaker, Alexander Dent. In response to the EuroPKI 2009 call for papers, a total of 40 submissions were received. All submissions underwent a thorough blind review by at least three ProgramCommittee members, resulting in careful selection and revision of the accepted papers. After the conference, the papers were revised and improved by the authors before inclusion in this volume.

Researchers in the ?eld of life sciences rely increasingly on information te- nology to extract and manage relevant knowledge. The complex computational and data management needs of life science research make Grid technologies an attractive support solution. However, many important issues must be addressed before the Life Science Grid becomes commonplace. The 1st International Life Science Grid Workshop (LSGRID 2004) was held in Kanazawa Japan, May 31–June 1, 2004. This workshop focused on life s- ence applications of grid systems especially for bionetwork research and systems biology which require heterogeneous data integration from genome to phenome, mathematical modeling and simulation from molecular to population levels, and high-performance computing including parallel processing, special hardware and grid computing. Fruitful discussions took place through 18 oral presentations, including a keynote address and ?ve invited talks, and 16 poster and demonstration p- sentations in the ?elds of grid infrastructure for life sciences, systems biology, massive data processing, databases and data grids, grid portals and pipelines for functional annotation, parallel and distributed applications, and life science grid projects. The workshop emphasized the practical aspects of grid techno- gies in terms of improving grid-enabled data/information/knowledge

sharing, high-performance computing, and collaborative projects. There was agreement among the participants that the advancement of grid technologies for life science research requires further concerted actions and promotion of grid applications. We therefore concluded the workshop with the announcement of LSGRID 2005.

This book is a tutorial on, and a guide to the deployment of, Public-Key Infrastructures. It covers a broad range of material related to PKIs, including certification, operational considerations and standardization efforts, as well as deployment issues and considerations. Emphasis is placed on explaining the interrelated fields within the topic area, to assist those who will be responsible for making deployment decisions and architecting a PKI within an organization.

This book contains the proceedings of the 2nd EuroPKI Workshop — EuroPKI 2005, held at the University of Kent in the city of Canterbury, UK, 30 June–1 July 2005. The workshop was informal and lively, and the university setting encouragedactive exchangesbetween the speakersand the audience. Theworkshopprogramcomprisedakeynotespeechfrom Dr. CarlisleAdams, followedby18refereedpapers,withaworkshopdinnerinandguidedtouraround the historic Dover Castle. Dr. Adams is well known for his contributions to the CAST family of s- metric encryption algorithms, to international standards from the IETF, ISO, and OASIS, authorship of over 30 refereed journals and conference papers, and co-authorship of Understanding PKI: Concepts, Standards, and Deployment Considerations (Addison-Wesley). Dr. Adams keynote speech was entitled 'PKI: Views from the Dispassionate "I",' in which he presented his thoughts on why PKIhas been availableas an authentication technology for many years now,but has only enjoyed large-scale success in fairly limited contexts to date. He also presented his thoughts on the possible future(s) of this technology, with emp- sis on the major factors hindering adoption and some potential directions for future research in these areas. In response to the Call for Papers, 43 workshop papers were submitted in total. All papers were blind reviewed by at least two members of the Program Committee, the majority having 3 reviewers, with a few borderline papers h- ing 4 or more reviewers; 18 papers were accepted for presentation in 8 sessions.

"This book reports on the latest advances in privacy protection issues and technologies for e-services, ranging from consumer empowerment to assess privacy risks, to security technologies needed for privacy protection, to systems for privacy policy enforcement, and even methods for assessing privacy technologies"--Provided by publisher.

This book discusses the implementation of privacy by design in Europe, a principle that has been codified within the European Data Protection Regulation (GDPR). While privacy by design inspires hope for future privacy-sensitive designs, it also introduces the need for a common understanding of the legal and technical concepts of privacy and data protection. By pursuing an interdisciplinary approach and comparing the problem definitions and objectives of both disciplines, this book bridges the gap between the legal and technical fields in order to enhance the regulatory and academic discourse. The research presented reveals the scope of legal principles and technical tools for privacy protection, and shows that the concept of privacy by design goes beyond the principle of the GDPR. The book presents an analysis of how current regulations delegate the implementation of technical privacy and data protection measures to developers and describes how policy design must evolve in order to implement

privacy by design and default principles.
Contains the latest research, case studies, theories, and methodologies within the field of wireless technologies.
Digital identity can be defined as the digital representation of the information known about a specific individual or organization. Digital identity management technology is an essential function in customizing and enhancing the network user experience, protecting privacy, underpinning accountability in transactions and interactions, and complying with regulatory controls. This practical resource offers you a in-depth understanding of how to design, deploy and assess identity management solutions. It provides a comprehensive overview of current trends and future directions in identity management, including best practices, the standardization landscape, and the latest research finding. Additionally, you get a clear explanation of fundamental notions and techniques that cover the entire identity lifecycle.
Recent advances in technology and new software applications are steadily transforming human civilization into what is called the Information Society. This is manifested by the new terminology appearing in our daily activities. E-Business, E-Government, E-Learning, E-Contracting, and E-Voting are just a few of the ever-growing list of new terms that are shaping the Information Society. Nonetheless, as "Information" gains more prominence in our society, the task of securing it against all forms of threats becomes a vital and crucial undertaking. Addressing the various security issues confronting our new Information Society, this volume is divided into 13 parts covering the following topics: Information Security Management; Standards of Information Security; Threats and Attacks to Information; Education and Curriculum for Information Security; Social and Ethical Aspects of Information Security; Information Security Services; Multilateral Security; Applications of Information Security; Infrastructure for Information Security Advanced Topics in Security; Legislation for Information Security; Modeling and Analysis for Information Security; Tools for Information Security. Security in the Information Society: Visions and Perspectives comprises the proceedings of the 17th International Conference on Information Security (SEC2002), which was sponsored by the International Federation for Information Processing (IFIP), and jointly organized by IFIP Technical Committee 11 and the Department of Electronics and Electrical Communications of Cairo University. The conference was held in May 2002 in Cairo, Egypt.
The ubiquity of modern technologies has allowed for increased connectivity between people and devices across the globe. This connected infrastructure of networks creates numerous opportunities for applications and uses. As the applications of the internet of things continue to progress so do the security concerns for this technology. The study of threat prevention in the internet of things is necessary as security breaches in this field can ruin industries and lives. Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications is a vital reference source that examines recent developments and emerging trends in security and privacy for the internet of things through new models, practical solutions, and technological advancements related to security. Highlighting a range of topics such as cloud security, threat detection, and open source software, this multi-volume book is ideally designed for engineers, IT consultants, ICT procurement managers, network system integrators, infrastructure service providers, researchers, academics, and professionals interested in current research on security practices pertaining to the internet

of things.

With most services and products now being offered through digital communications, new challenges have emerged for information security specialists. A Multidisciplinary Introduction to Information Security presents a range of topics on the security, privacy, and safety of information and communication technology. It brings together methods in pure mathematics, computer and telecommunication sciences, and social sciences. The book begins with the cryptographic algorithms of the Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA). It explains the mathematical reasoning behind public key cryptography and the properties of a cryptographic hash function before presenting the principles and examples of quantum cryptography. The text also describes the use of cryptographic primitives in the communication process, explains how a public key infrastructure can mitigate the problem of crypto-key distribution, and discusses the security problems of wireless network access. After examining past and present protection mechanisms in the global mobile telecommunication system, the book proposes a software engineering practice that prevents attacks and misuse of software. It then presents an evaluation method for ensuring security requirements of products and systems, covers methods and tools of digital forensics and computational forensics, and describes risk assessment as part of the larger activity of risk management. The final chapter focuses on information security from an organizational and people point of view. As our ways of communicating and doing business continue to shift, information security professionals must find answers to evolving issues. Offering a starting point for more advanced work in the field, this volume addresses various security and privacy problems and solutions related to the latest information and communication technology.

Over the past years, Public Key Infrastructure (PKI) technology has evolved and moved from the research laboratories to the mainstream, in which many organizations are now leveraging it as part of their core infrastructure system for providing and building security in their businesses. Understanding the challenges and requirements of PKI related operations through the sharing of case studies are critical to supporting the continued research and development of PKI technologies and related systems and applications to further progress and innovate for enhancing future development and evolution of PKI in the enterprises. This publication includes topics such as: PKI Operation & Case Study; Non-repudiation; Authorization & Access Control, Authentication & Time-Stamping, Certificate Validation & Revocation and Cryptographic Applications.

"This book provides an overall view of trust for e-services including definitions, constructs, and relationships with other research topics such as security, privacy, reputation and risk. It offers contributions from real-life experience and practice on how to build a trust environment for e-government services"--Provided by publisher.

This volume constitutes the refereed proceedings of the 6th International Conference on Multimedia Communications, Services and Security, MCSS 2013, held in Krakow, Poland, in June 2013. The 27 full papers included in the volume were selected from numerous submissions. The papers cover various topics related to multimedia technology and its application to public safety problems.

"This book investigates various definitions of trust and their characteristics in distributed systems and digital computing, and details how to model and implement trust in a digital system"--Provided by publisher.

ICICS 2003, the Fifth International Conference on Information and C- munication Security, was held in Huhehaote city, Inner Mongolia,

China, 10–13 October 2003. Among the preceding conferences, ICICS'97 was held in B- jing, China, ICICS'99 in Sydney, Australia, ICICS 2001 in Xi'an, China, and ICICS 2002,in Singapore.TheproceedingswerereleasedasVolumes1334,1726, 2229, and 2513 of the LNCS series of Springer-Verlag, respectively. ICICS 2003 was sponsored by the Chinese Academy of Sciences (CAS), the National Natural Science Foundation of China, and the China Computer F- eration. The conference was organized by the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences (ERCIST, CAS) in co-operation with the International Communications and Information Security Association (ICISA). The aim of the ICICS conferences has been to o?er the attendees the - portunity to discuss the state-of-the-art technology in theoretical and practical aspects of information and communications security. The response to the Call forPaperswassurprising.WhenwewerepreparingtheconferencebetweenApril and May, China, including the conference venue, Huhehaote City, was ?ghting against SARS. Despite this 176 papers were submitted to the conference from 22 countries and regions, and after a competitive selection process, 37 papers from 14 countries and regions were accepted to appear in the proceedings and be presented at ICICS 2003. We would like to take this opportunity to thank all those who submitted papers to ICICS 2003 for their valued contribution to the conference.

ROADMAP TO INFORMATION SECURITY: FOR IT AND INFOSEC MANAGERS provides a solid overview of information security and its relationship to the information needs of an organization. Content is tailored to the unique needs of information systems professionals who find themselves brought in to the intricacies of information security responsibilities. The book is written for a wide variety of audiences looking to step up to emerging security challenges, ranging from students to experienced professionals. This book is designed to guide the information technology manager in dealing with the challenges associated with the security aspects of their role, providing concise guidance on assessing and improving an organization's security. The content helps IT managers to handle an assignment to an information security role in ways that conform to expectations and requirements, while supporting the goals of the manager in building and maintaining a solid information security program. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book offers a comprehensive understanding of secure Internet messaging, and brings together all the relevant and critical information needed to use OpenPGP and S/MIME-compliant software. It explores the conceptual and technical approaches followed by the developers of both OpenPGP and S/MIME, and gives a thorough treatment of the latest and most-effective technologies for secure messaging. Ideal for security and network managers, as well as professional system and network administrators, this easy-to-understand book is a complete guide to OpenPGP, S/MIME, Web-based and gateway solutions, certified mail, delivery platforms, and instant messaging.