Computer Security 3rd Edition Dieter Gollmann

Computer SecurityJohn Wiley & Sons

This volume constitutes the proceedings of the Third European Symposium on Research in Computer Security, held in Brighton, UK in November 1994. The 26 papers presented in the book in revised versions were carefully selected from a total of 79 submissions; they cover many current aspects of computer security research and advanced applications. The papers are grouped in sections on high security assurance software, key management, authentication, digital payment, distributed systems, access control, databases, and measures.

As the computer industry moves into the 21st century, the long-running Advances in Computers is ready to tackle the challenges of the new century with insightful articles on new technology, just as it has since 1960 in chronicling the advances in computer technology from the last century. As the longest-running continuing series on computers, Advances in Computers presents those technologies that will affect the industry in the years to come. In this volume, the 53rd in the series, we present 8 relevant topics. The first three represent a common theme on distributed computing systems -using more than one processor to allow for parallel execution, and hence completion of a complex computing task in a minimal amount of time. The other 5 chapters describe other relevant advances from the late 1990s with an emphasis on software development, topics of vital importance to developers today- process improvement, measurement and legal liabilities. Key Features * Longest running series on computers * Contains eight insightful chapters on new technology * Gives comprehensive treatment of distributed systems * Shows how to evaluate measurements * Details how to evaluate software process improvement models * Examines how to expand e-commerce on the Web * Discusses legal liabilities in developing software—a must-read for developers

Research on Secure Key Establishment has become very active within the last few years. Secure Key Establishment discusses the problems encountered in this field. This book also introduces several improved protocols with new proofs of security. Secure Key Establishment identifies several variants of the key sharing requirement. Several variants of the widely accepted Bellare and Rogaway (1993) model are covered. A comparative study of the relative strengths of security notions between these variants of the Bellare–Rogaway model and the Canetti–Krawczyk model is included. An integrative framework is proposed that allows protocols to be analyzed in a modified version of the Bellare–Rogaway model using the automated model checker tool. Secure Key Establishment is designed for advanced level students in computer science and mathematics, as a secondary text or reference book. This book is also suitable for practitioners and researchers working for defense agencies or security companies.

Describes how to put software security into practice, covering such topics as risk management frameworks, architectural risk analysis, security testing, and penetration testing.

Cryptographic Primitives in Blockchain Technology provides an introduction to the mathematical and cryptographic concepts behind blockchain technologies and shows how they are applied in blockchain-based systems.

Insider Threats in Cyber Security is a cutting edge text presenting IT and non-IT facets of insider threats together. This volume brings together a critical mass of well-established worldwide researchers, and provides a unique multidisciplinary overview. Monica van Huystee, Senior Policy Advisor at MCI, Ontario, Canada comments "The book will be a must read, so of course I'll need a copy." Insider Threats in Cyber Security covers all aspects of insider threats, from motivation to mitigation. It includes how to monitor insider threats (and what to monitor for), how to mitigate insider threats, and related topics and case studies. Insider Threats in Cyber Security is intended for a professional audience composed of the military, government policy makers and banking; financing companies focusing on the Secure Cyberspace industry. This book is also suitable for advanced-level students and researchers in computer science as a secondary text or reference book.

This book constitutes the refereed proceedings of the 5th European Symposium on Research in Computer Security, ESORICS 98, held in Louvain-la-Neuve, Belgium, in September 1998. The 24 revised full papers presented were carefully reviewed and selected from a total of 57 submissions. The papers provide current results from research and development in design and specification of security policies, access control modelling and protocol analysis, mobile systems and anonymity, Java and mobile code, watermarking, intrusion detection and prevention, and specific threads.

Foreword from the Program Chairs These proceedings contain the papers selected for presentation at the 10th - ropean Symposium on Research in Computer Security (ESORICS), held S- tember 12–14, 2005 in Milan, Italy. In response to the call for papers 159 papers were submitted to the conf- ence. These paperswere evaluated on the basis of their signi?cance, novelty,and technical quality. Each paper was reviewed by at least three members of the program committee. The program committee meeting was held electronically, holding intensive discussion over a period of two weeks. Of the papers subm- ted, 27 were selected for presentation at the conference, giving an acceptance rate of about 16%. The conference program also includes an invited talk by Barbara Simons. There is a long list of people who volunteered their time and energy to put together the symposiom and who deserve acknowledgment. Thanks to all the members of the program committee, and the external reviewers, for all their hard work in evaluating and discussing papers. We are also very grateful to all those people whose work ensured a smooth organizational process: Pierangela Samarati, who served as General Chair, Claudio Ardagna, who served as P- licity Chair, Dieter Gollmann who served as Publication Chair and collated this volume, and Emilia Rosti and Olga Scotti for helping with local arrangements. Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you ?nd the program stimulating.

This book constitutes the refereed proceedings of the 9th European Symposium on Research in Computer Security, ESORICS 2004, held in Sophia Antipolis, France in September 2004. The 27 revised full papers presented were carefully reviewed and selected from 159 submissions. Among the topics addressed are access control, authorization frameworks, privacy policies, security protocols, trusted computing, anonymity, information hiding, steganography, digital signature schemes, encrypted communication, information flow control, authentication, key distribution, public key cryptography, intrusion prevention, and attack discovery.

The definitive book on UNIX security, this volume covers every aspect of computer security on UNIX machines and the Internet.

ESORICS, the European Symposium on Research in Computer Security, is the leading research-oriented conference on the theory and practice of computer security in Europe. It takes place every two years, at various locations throughout Europe, and is coordinated by an independent Steering Committee. ESORICS 2002 was jointly organized by the Swiss Federal Institute of Te- nology (ETH) and the IBM Zurich Research Laboratory, and took place in Zurich, Switzerland, October 14-16, 2002. The program committee received 83 submissions, originating from 22 co- tries. For fans of statistics: 55 submissions came from countries in Europe, the Middle East, or Africa, 16 came from Asia, and 12from North America. The leading countries were USA (11 submissions), Germany (9), France (7), Italy (7), Japan (6), and UK (6). Each submission was reviewed by at least three p- gram committee members or other experts. Each submission coauthored by a program committee member received two additional reviews. The program c- mittee chair and cochair were not allowed to submit papers. The ?nal selection of papers was made at a program committee meeting and resulted in 16 accepted papers. In comparison, ESORICS 2000 received 75 submissions and accepted 19 of them. The program re?ects the full range of security research: we accepted papers on access control, authentication, cryptography, database security, formal methods, intrusion detection, mobile code security, privacy, secure hardware, and secure protocols. We gratefully acknowledge all authors who submitted papers for their e?orts in maintaining the standards of this conference.

ICICS'99, the Second International Conference on Information and C- munication Security, was held in Sydney, Australia, 9-11 November 1999. The conference was sponsored by the Distributed System and Network Security - search Unit, University of Western Sydney, Nepean, the Australian Computer Society, IEEE Computer Chapter (NSW), and Harvey World Travel. I am g- teful to all these organizations for their support of the conference. The conference brought together researchers, designers, implementors and users of information security systems and technologies. A range of aspects was addressed from security theory and modeling to system and protocol designs and implementations to applications and management. The conference con- sted of a series of refereed technical papers and invited technical presentations. The program committee invited two distinguished key note speakers. The ?rst keynote speech by Doug McGowan, a Senior Manager from Hewlett-Packard, USA, discussed cryptography in an international setting. Doug described the current status of international cryptography and explored possible future trends and new technologies. The second keynote speech was delivered by Sushil Ja- dia of George Mason University, USA. Sushil's talk addressed the protection of critical information systems. He discussed issues and methods for survivability of systems under malicious attacks and proposed a fault-tolerance based - proach. The conference also hosted a panel on the currently much debated topic of Internet censorship. The panel addressed the issue of censorship from various viewpoints namely legal, industrial, governmental and technical.

This text examines computer security and privacy. It covers topics such as: access control; information flow; covert channels; secure protocols; database security; verification techniques; and integrity and availability models.

The modern society is rapidly becoming a fully digital society. This has many benefits, but unfortunately it also means that personal privacy is threatened. The threat does not so much come from a 1984 style Big Brother, but rather from a set of smaller big brothers. The small big brothers are companies that we interact with; they are public services and institutions. Many of these little big brothers are indeed also being invited to our private data by ourselves. Privacy as a subject can be problematic. At the extreme it is personal freedom against safety and security. We shall not take a political stand on personal privacy and what level of personal freedom and privacy is the correct one. Aspects of Personal Privacy in Communications is mostly about understanding what privacy is and some of the technologies may help us to regain a bit of privacy. We discuss what privacy is about, what the different aspects of privacy may be and why privacy needs to be there by default. There are boundaries between personal privacy and societal requirements, and inevitably society will set limits to our privacy (Lawful Interception, etc.). There are technologies that are specifically designed to help us regain some digital privacy. These are commonly known as Privacy Enhancing Technologies (PETs). We investigate some these PETs including MIX networks, Onion Routing and various privacy-preserving methods. Other aspects include identity and location privacy in cellular systems, privacy in RFID, Internet-of-Things (IoT) and sensor networks amongst others. Some aspects of cloud systems are also covered. Content: Getting a Grip on Privacy The Legal Context of Privacy Anonymous Communications Secure Multi-party Computations and Privacy Privacy and Data Mining in Telecommunications Requirements for Cellular System Subscriber Privacy The 3GPP Systems and Subscriber Privacy Future Cellular Systems and Enhanced Subscriber Privacy Sensor Networks Radio Frequency Identification Privacy and Trust for the Internet-of-Things Privacy in the Cloud Summary and Concluding Remarks

This book constitutes the refereed proceedings of the 5th International Conference on Information and Communication Security, ICICS 2003, held in Huhehaote, China, in October 2003. The 37 revised full papers presented were carefully reviewed and selected from 176 submissions. The papers address a broad variety of topics in information and communications security including finite field computations, digital signature schemes, mobile agents security, access control, cryptographic attacks, public key cryptography, peer-to-peer security, watermarking, broadcast encryption, information hiding, cryptographic protocols, oblivious transfer, fingerprinting schemes, security verification, TCP/IP security, support vector machine, intrusion detection, and authenticated encryption schemes.

This new book is a clearly written, well structured guide to building secure distributed applications with CORBA. It helps securing CORBA applications, integrating security infrastructure with CORBA applications, and evaluating the security effectiveness of distributed applications. You get a comprehensive study of the CORBA security architecture, providing you with a better understanding of its goals and limitations. It serves as your complete reference for understanding security in distributed systems.

This book constitutes the refereed proceedings of the Third International Workshop on Information Security, ISW 2000, held in Wollongong, Australia in December 2000. The 23 revised full papers presented were carefully reviewed and selected from 63 submissions. The papers are organized in topical sections on multimedia copyright protection, e-commerce, key management, network security and access control, and cryptographic systems.

Safety and Reliability of Software Based Systems contains papers, presented at the twelfth annual workshop organised by the Centre for Software Reliability. Contributions come from different industries in many countries, and provide discussion and cross-fertilisation of ideas relevant to systems whose safety and/or reliability are of paramount concern. This book discusses safety cases and their varying roles in different industries; using measurement to improve reliability and safety of software-based systems; latest developments in managing, developing and assessing software intensive systems where reliability and/or safety are important considerations; and practical experiences of others in industry.

Security Education and Critical Infrastructures presents the most recent developments in research and practice on teaching information security, and covers topics including: -Curriculum design; -Laboratory systems and exercises; -Security education program assessment; -Distance learning and web-based teaching of security; -Teaching computer forensics; -Laboratory-based system defense games; -Security education tools; -Education in security policies, management and system certification; -Case studies.
??????????????????????3???
>
his book presents the refereed proceedings of the 6th European Symposium on Research in Computer Security, ESORICS 2000, held in Toulouse, France in October 2000. The 19 revised full papers presented were carefully reviewed and selected from a total of 75 submissions. The papers are organized in sections on personal devices and smart cards, electronic commerce protocols, access control, protocol verification, Internet security, security property analysis, and mobile agents.

Law of the Internet, Fourth Edition is a two-volume up-to-date legal resource covering electronic commerce and online contracts, privacy and network security, intellectual property and online content management, secure electronic transactions, cryptography, and digital signatures, protecting intellectual property online through link licenses, frame control and other methods, online financial services and securities transactions, antitrust and other liability. The Law of the Internet, Fourth Edition quickly and easily gives you everything you need to provide expert counsel on: Privacy laws and the Internet Ensuring secure electronic transactions, cryptography, and digital signatures Protecting intellectual property online - patents, trademarks, and copyright Electronic commerce and contracting Online financial services and electronic payments Antitrust issues, including pricing, bundling and tying Internal network security Taxation of electronic commerce Jurisdiction in Cyberspace Defamation and the Internet Obscene and indecent materials on the Internet Regulation of Internet access and interoperability The authors George B. Delta and Jeffrey H. Matsuura -- two Internet legal experts who advise America's top high-tech companies -- demonstrate exactly how courts, legislators and treaties expand traditional law into the new context of the Internet and its commercial applications, with all the citations you'll need. The Law of the Internet also brings you up to date on all of the recent legal, commercial, and technical issues surrounding the Internet and provides you with the knowledge to thrive in the digital marketplace. Special features of this two-volume resource include timesaving checklists and references to online resources.

One of a firm's most valuable resources is its data: client lists, accounting data, employee information, and so on. This critical data must be securely managed and controlled, and simultaneously made available to those users authorized to see it. The IBM® z/VSE® system features extensive capabilities to simultaneously share the firm's data among multiple users and protect them. Threats to this data come from various sources. Insider threats and malicious hackers are not only difficult to detect and prevent, they might be using resources with the business being unaware. This IBM Redbooks® publication was written to assist z/VSE support and security personnel in providing the enterprise with a safe, secure and manageable environment. This book provides an overview of the security that is provided by z/VSE and the processes for the implementation and configuration of z/VSE security components, Basic Security Manager (BSM), IBM CICS® security, TCP/IP security, single sign-on using LDAP, and connector security.

With the rapid development of information technologies and the transition to next-generation networks, computer systems and in particular embedded s- tems are becoming more and more mobile and ubiquitous. They also strongly interact with the physical world. Ensuring the security of these complex and resource-constrained systems is a really challenging research topic. Therefore this Workshop in Information Security Theory and Practices was organized to bring together researchers and practitioners in related areas, and to encourage cooperation between the research and the industrial communities. This was the second edition of WISTP, after the ?rst event in Heraklion, Greece, in 2007. This year again we had a signi?cant number of high-quality submissions coming from many di?erent countries. These submissions re?ected the major topics of the conference, i. e. , smart devices, convergence, and ne- generation networks. Submissions were reviewed by at least three reviewers, in most cases by four, and at least by ?ve for the papers involving Program C- mittee members. This long and rigorousprocess could be achievedthanks to the hard work of the Program Committee members and additional reviewers, listed in the following pages. This led to the selection of high-quality papers that made up the workshop program and are published in these proceedings. A number of posters and short papers were also selected for presentation at the conference. The process was very selective and we would like to thank all those authors who submitted contributions that could not be selected.

Written for people who manage information security risks for their organizations, this book details a security risk evaluation approach called "OCTAVE." The book provides a framework for systematically evaluating and managing security risks, illustrates the implementation of self-directed evaluations, and shows how to tailor evaluation methods to the needs of specific organizations. A running example illustrates key concepts and techniques. Evaluation worksheets and a catalog of best practices are included. The authors are on the technical staff of the Software Engineering Institute. Annotation copyrighted by Book News, Inc., Portland, OR

"This 10-volume compilation of authoritative, research-based articles contributed by thousands of researchers and experts from all over the world emphasized modern issues and the presentation of potential opportunities, prospective solutions, and future directions in the field of information science and technology"--Provided by publisher.

Protocols for authentication and key establishment are the foundation for security of communications. The range and diversity of these protocols is immense, while the properties and vulnerabilities of different protocols can vary greatly. This is the first comprehensive and integrated treatment of these protocols. It allows researchers and practitioners to quickly access a protocol for their needs and become aware of existing protocols which have been broken in the literature. As well as a clear and uniform presentation of the protocols this book includes a description of all the main attack types and classifies most protocols in terms of their properties and resource requirements. It also includes tutorial material suitable for graduate students.

This book constitutes the refereed proceedings of the 9th International Conference on Information Security, ISC 2006, held on Samos Island, Greece in August/September 2006. The 38 revised full papers presented were carefully reviewed and selected from 188 submissions. The papers are organized in topical sections.

This book constitutes the refereed proceedings of the 15th International Conference on Information Security, ISC 2015, held in Passau, Germany, in September 2012. The 23 revised full papers presented together with one invited paper were carefully reviewed and selected from 72 submissions. The papers are organized in topical sections on cryptography and cryptanalysis, mobility, cards and sensors, software security, processing encrypted data, authentication and identification, new directions in access control, GPU for security, and models for risk and revocation.

A completely up-to-date resource on computer security Assuming no previous experience in the field of computer security, this must-have book walks you through the many essential aspects of this vast topic, from the newest advances in software and technology to the most recent information on Web applications security. This new edition includes sections on Windows NT, CORBA, and Java and discusses cross-site scripting and JavaScript hacking as well as SQL injection. Serving as a helpful introduction, this self-study guide is a wonderful starting point for examining the variety of competing security systems and what makes them different from one another. Unravels the complex topic of computer security and breaks it down in such a way as to serve as an ideal introduction for beginners in the field of computer security Examines the foundations of computer security and its basic principles Addresses username and password, password protection, single sign-on, and more Discusses operating system integrity, hardware security features, and memory Covers Unix security, Windows security, database security, network security, web security, and software security Packed with in-depth coverage, this resource spares no details when it comes to the critical topic of computer security.

The two-volume set, LNCS 10492 and LNCS 10493 constitutes the refereed proceedings of the 22nd European Symposium on Research in Computer Security, ESORICS 2017, held in Oslo, Norway, in September 2017. The 54 revised full papers presented were carefully reviewed and selected from 338 submissions. The papers address issues such as data protection; security protocols; systems; web and network security; privacy; threat modeling and detection; information flow; and security in emerging applications such as cryptocurrencies, the Internet of Things and automotive.

This book constitutes the refereed proceedings of the 11th European Symposium on Research in Computer Security, ESORICS 2006. The 32 revised full papers presented were carefully reviewed and selected from 160 submissions. ESORICS is confirmed as the European research event in computer security; it presents original research contributions, case studies and implementation experiences addressing any aspect of computer security - in theory, mechanisms, applications, or practical experience.

This book constitutes the refereed proceedings of the 8th European Symposium on Research in Computer Security, ESORICS 2003, held in Gjovik, Norway in October 2003. The 19 revised full papers presented were carefully reviewed and selected from 114 submissions. Among the topics addressed are signature control, access control, key exchange, broadcast protocols, privacy preserving technologies, attack analysis, electronic voting, identity control, authentication, security services, smart card security, formal security protocols analysis, and intrusion detection.