E-COMMERCE SECURITY AND PRIVACY

ADVANCES IN INFORMATION SECURITY

Additional titles in the series:

INFORMATION HIDING: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, and Sushil Jajodia
ISBN: 0-7923-7204-2

RECENT ADVANCES IN RSA CRYPTOGRAPHY *by Stefan Katzenbeisser*
ISBN: 0-7923-7438-X

E-COMMERCE SECURITY AND PRIVACY

edited by

Anup K. Ghosh
Cigital, Inc., U.S.A.

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Library of Congress Cataloging-in-Publication Data

E-commerce security and privacy / edited by Anup K. Ghosh.
p. cm. — (Advances in information security ; 2)
Includes bibliographical references and index.
ISBN 978-1-4613-5568-7 ISBN 978-1-4615-1467-1 (eBook)
DOI 10.1007/978-1-4615-1467-1
1. Computer security. 2. Privacy, Right. 3. E-commerce—Security measures. I. Ghosh, Anup K. II. Series.

QA76.9.A25 R433 2001
005.8—dc2

2001034439

Printed on acid-free paper.

Contents

List of Figures

List of Tables

Contributing Authors

Annie I. Antón is the Asea Brown Boveri Assistant Professor of Software Engineering in the North Carolina State University College of Engineering. She is Co-Director of the NC State E-Commerce Studio, recipient of an NSF CAREER Award, and a member of the IEEE and the ACM.

Brad Arkin is a founding member of the Software Security Group at Cigital, Inc. He helps Cigital's clients build and operate security critical software.

Mikhail J. Atallah is a professor in the Computer Sciences Department at Purdue University. Dr. Atallah received a BE degree in electrical engineering from the American University, Beirut, Lebanon, in 1975, and MS and Ph.D. degrees in electrical engineering and computer science from Johns Hopkins University, Baltimore, Maryland, in 1980 and 1982, respectively.

Andre Dos Santos joined the Georgia Tech College of Computing faculty in the fall of 2000 as an Assistant Professor. His research interests are in all aspects of computer security, but focus particularly on the security and use of tamper resistant devices such as smart cards, the security of Internet technologies and applications, and the security of online banking systems and online brokerage.

Wenliang Du is currently a Ph.D. student in the Department of Computer Sciences and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University.

Julia B. Earp is an Assistant Professor in the North Carolina State University College of Management. She is Co-Director of the NC State

E-Commerce Studio, Director of the NCSU Internet Security and Privacy Project and is a member of the IEEE and ACM.

Anup K. Ghosh is Director of Security Research at Cigital, Inc. He is author of *Security and Privacy for E-Business* (Wiley, 2001) and *E-Commerce Security: Weak Links, Best Defenses* (Wiley, 1998).

Marc Goodman is the Chief Cybercriminologist for the information security consultancy AtomicTangerine. Mr. Goodman is a member of Interpol's global steering committee on information technology crime and is the former Officer-in-Charge of the Los Angeles Police Department's Internet Unit.

Sushil Jajodia is BDM Professor and Chairman of the Department of Information and Software Engineering and Director of Center for Secure Information Systems at the George Mason University, Fairfax, Virginia. His email address is jajodiagmu.edu and the his web page address is http://isse.gmu.edu/ csis/faculty/jajodia.html.

Richard A. Kemmerer is a Professor and past Chair of the Department of Computer Science at the University of California, Santa Barbara. His research interests include formal specification and verification of systems, computer system security and reliability, programming and specification language design, and software engineering.

Michiharu Kudo received the B.E. degree and M.E. degree from Tokyo University, Tokyo, Japan, in 1986 and 1988, respectively. He is currently a researcher at IBM Tokyo Research Laboratory.

V.S. Subrahmanian is Professor of Computer Science at the University of Maryland, College Park. He has worked extensively on heterogeneous data and software integration, software agents, multimedia databases, probabilistic and temporal databases, and computational logic systems.

Vijay Varadharajan is Microsoft Chair Professor of Computing at Macquarie University and is the Director of Information and Networked Systems Security Research. He is also the Technical Board Director of Australian Computer Society.

Giovanni Vigna is an Assistant Professor in the Department of Computer Science at the University of California in Santa Barbara. His current research interests include network and computer security, intrusion detection systems, security of mobile code systems, penetration testing, and distributed systems.

Hongxue Wang is an associate professor at Athabasca University, Canada. His areas of interest include intelligent system modeling, electronic commerce, computer security, and distance education.

Yan Zhang is a senior lecturer at University of Western Sydney, Australia. His research interests include logic and knowledge-based systems.

Foreword

Welcome to the second volume of the Kluwer International Series on ADVANCES IN INFORMATION SECURITY. The goals of this series are, one, to establish the state of the art of and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

The success of this series depends on contributions by researchers and developers such as yourself. If you have an idea for a book that is appropriate for this series, I encourage you to contact either the Acquisitions Editor for the series, Lance Wobus (lwobus@wkap.com), or myself, the Consulting Editor for the series (jajodia@gmu.edu). We would be happy to discuss any potential projects with you. Additional information about this series can be obtained from www.wkap.nl/series.htm/ADIS.

About this volume

The second volume of this series is entitled *Recent Advances in E-Commerce Security and Privacy*, edited by Anup K. Ghosh.

Electronic commerce represents a tremendous opportunity and difficult challenge for security researchers and practitioners. Business-to-consumer (B2C) and business-to-business (B2B) applications are rapidly changing the way we conduct business these days. However, how we can do this while protecting both businesses and consumers from theft and false representation continues to be an open problem. Solutions that are being deployed in the marketplace have often been ad hoc in nature, and there is a need to provide a principled theoretical foundation. This volume brings together contributions from a number of respected researchers to address this need.

It has been a pleasure working with the editor of this volume, Anup K. Ghosh, who is a world-renowned expert in electronic commerce security. He is a noted speaker and the author of *Security and Privacy for E-Business* (Wiley, 2001) and *E-Commerce Security: Weak Links, Best Defenses* (Wiley, 1998).

SUSHIL JAJODIA
Consulting Editor

Preface

The Internet has fundamentally changed much of the way most of us do business now. Electronic commerce (or e-commerce) in its many myriad forms utilizes technology to connect people and facilitate business. Business-to-business e-commerce transactions are expected to exceed US $6 trillion by 2006. Perhaps more revealing of how e-commerce is changing the commercial landscape is that e-commerce transactions are expected to account for 25% of all retail transactions in the next decade.

Throughout the period of meteoric growth in e-commerce, the security risks have grown similarly in scope and magnitude. Three major factors have driven the security risks in e-commerce: first, the sole reliance on the electronic medium for a company's core business, second, the growing complexity of the software systems needed to support e-commerce, and third, the value of the digital assets brought online to an inherently insecure medium — the Internet.

While security has long been a primary concern in e-commerce, more recently, *privacy* concerns have become the number one concern for consumers. Many of the same Internet technologies that make e-commerce possible, also make it possible to create detailed profiles of an individual's purchases, to spy on individual Web usage habits, and even to peer into confidential files that reside on the individual's machine.

While much has been written in the popular literature about electronic commerce risks, this volume is the first to pull together leading researchers and practitioners in different fields of computer science and software engineering to present their technical innovations to problems in security and privacy in e-commerce. This book draws from selected papers presented at the first Workshop on Security and Privacy in E-Commerce (WSPEC'00) held in Athens, Greece, November 4, 2000. The papers were selected for their quality and also for the breadth in topics in e-commerce security and privacy they represent.

The book is divided into two parts: (1) selected case studies in electronic commerce security, and (2) reasoning about secure and private electronic commerce. The first part is aimed at the practitioner who seeks understanding and insight into problems encountered in electronic commerce security and privacy as well as practical solutions.

In the first part of the book, we present two case studies on analyzing the security of e-commerce systems. The first case study assumes no first hand knowledge of the software that runs an online banking system, while the second provides a case study into working with an organization and its software to identify and mitigate problems in an online gambling operation. The third case study examines new problems that arise in mobile e-commerce — an emerging field that is taking advantage of wireless Internet connectivity to handheld devices. The final case study examines the technical and legal problems facing law enforcement in identifying and prosecuting transnational computer crimes. The case study shows that while the Internet knows no geographic boundaries, law enforcement is faced with considerable jurisdictional hurdles in tracking and prosecuting malicious hackers.

The second part of this book is more formal and is aimed at the researcher interested in state-of-the-art innovations in reasoning about secure and private e-commerce. Many of the articles in this section provide a framework about which to reason how a given protocol or system of e-commerce meets security and privacy requirements.

The first article in the second part provides a goal-based approach for specifying security and policy requirements into operational system requirements. The second article in this part addresses a timely issue: how to ensure secure and private access to Internet databases. The authors provide several protocols for secure remote access to online databases aimed at providing secure and private transactions for very confidential queries, such as to medical databases. The third article in this part provides a logic system for reasoning about accountabilities in cryptographic protocols for e-commerce. The final article provides a logic system for provisional authorizations in e-commerce transactions. The authors demonstrate the utility of provisional authorization to two types of e-commerce systems: electronic auctions and business-to-business e-commerce transactions.

In summary, this book provides both practitioners and researchers with innovations in secure and private e-commerce. Practitioners will gain great insight from the case studies, and researchers will be able to learn about state-of-the-art protocols in secure and private e-commerce that will serve as the basis for future innovations in applied e-commerce technologies.

Since the book is a collection or articles, the reader can jump straight to the chapters of interest without losing context from earlier chapters.

Speaking on behalf of all contributing authors, we believe the innovations contained in this book will blaze the trail for a more secure and private system of e-commerce in the future.

ANUP K. GHOSH

Acknowledgments

This book is a compilation of articles from many contributors. The contributors deserve much credit and appreciation for their time and dedication to preparing these articles for publication.

There were many individuals who also helped pull together the first Workshop on Security and Privacy in E-Commerce in Athens, Greece, from which selected papers were chosen for this volume. Foremost among them, Dimitris Gritzalis from the Athens University of Economics & Business deserves much credit for hosting and pulling together the workshop. In addition, this workshop was in large part the brainchild of Sushil Jajodia of George Mason University. The arduous efforts of the program committee in reviewing and selecting papers presented in the workshop also deserve much credit: Yair Frankel, Dimitris Gritzalis, Sushil Jajodia, Nikos Kyrloglou, Gary McGraw, Fabian Monrose, Pierangela Samarati, Tomas Sander, Sang Son, Bhavani Thuraisingham, Win Treese, Vijay Varadharajan, and Giovanni Vigna.

Finally, those who support us both at home and at work probably deserve the most credit for making possible the contributions in this book. We thank you all for your continued support.