SECURE ELECTRONIC VOTING

Advances in Information Security

Sushil Jajodia
Consulting editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of Kluwer International Series on ADVANCES IN INFORMATION SECURITY 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.

Researchers as well as developers are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

APPLICATIONS OF DATA MINING IN COMPUTER SECURITY, edited by Daniel Barbará, Sushil Jajodia; ISBN: 1-4020-7054-3
MOBILE COMPUTATION WITH FUNCTIONS by Zeliha Dilsun Kırlı, ISBN: 1-4020-7024-1
TRUSTED RECOVERY AND DEFENSIVE INFORMATION WARFARE by Peng Liu and Sushil Jajodia, ISBN: 0-7923-7572-6
RECENT ADVANCES IN RSA CRYPTOGRAPHY by Stefan Katzenbeisser, ISBN: 0-7923-7438-X
E-COMMERCE SECURITY AND PRIVACY by Anup K. Ghosh, ISBN: 0-7923-7399-5
INFORMATION HIDING: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, and Sushil Jajodia, ISBN: 0-7923-7204-2

Additional information about this series can be obtained from
www.wkap.nl/series.htm/ADIS.

SECURE
ELECTRONIC VOTING

edited by

Dimitris A. Gritzalis
Athens University of Economics and Business, Greece

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

Gritzalis, Dimitris A.
SECURE ELECTRONIC VOTING
ISBN 978-1-4613-4981-5 ISBN 978-1-4615-0239-5 (eBook)
DOI 10.1007/978-1-4615-0239-5

Originally published by Kluwer Academic Publishers in 2003
Softcover reprint of the hardcover 1st edition 2003

Printed on acid-free paper.

Contents

Part III Capabilities and Limitations

Contributing Authors

(in alphabetical order)

Danilo Bruschi is an Associate Professor of Computer Science with the Dept. of Information Science of the University of Milan. His research interests focus on computer and network security, operating systems, computer networks, and distributed systems. He is the Scientific Director of the *True-Vote* project (realization of a polling system for Internet), which is sponsored by the IST Programme of the European Union.

Mike Burmester is a Professor of Computer Science at Florida State University. Earlier, he was at Royal Holloway, London University. He got his BSc from University of Athens, and PhD from Rome University. His interests include privacy, anonymity, network security and watermarking.

Lorrie Faith Cranor is a Principal Technical Staff Member in the Secure Systems Research Department at AT&T Labs-Research. She has been studying electronic voting systems since 1994. In 2000 she served on the Executive Committee of a United States National Science Foundation sponsored Internet voting taskforce.

David Chaum received a PhD from the University of California at Berkeley. He taught, led a crypto research group, and founded DigiCash. He is widely recognized as the inventor of electronic cash; he was also the first to show how network voting could be private and secure. In 2000 he began developing new innovations for automated elections.

Ivan Damgård holds a PhD in Computer Science (1988). He has held a post -doctoral position at the Dept. of Computer Science of Aarhus University, where he currently is an Associate Professor, heading the Department's Research Group on Cryptography. He is a co-founder/co-owner of Cryptomathic A/S, and the author of about 100 research papers.

Ed Gerck holds a PhD in Physics from Ludwig-Maximilians University and Max-Planck Institute for Quantum Optics, Munich. He is the CEO of Safevote, Inc. His work in Internet security, cryptography, and voting received press coverage from New York Times, Le Monde, O'Globo, Forbes, Wired, CNN, CBS, Business Week, and USA Today.

Dimitris Gritzalis holds a PhD in Informatics (1994). He is an Assistant Professor of I&CT Security, with the Dept. of Informatics of the Athens University of Economics and Business, where he leads the Infosec Research Group. He is an Associate Data Protection Commissioner of Greece, and a Managing Board Member of the *e-vote* project of the European Commission.

Jens Groth holds an MSc in Mathematics from the University of Aarhus (2001). Currently he is working at Cryptomathic A/S and pursuing a PhD in Cryptography at BRICS, Dept. of Computer Science, University of Aarhus. His research interests include zero-knowledge proofs and electronic voting.

Spyros Ikonomopoulos holds an MSc in Information Systems from the Athens University of Economics and Business. He is a PhD candidate with the Dept. of Information and Communication Systems Engineering of the University of the Aegean. His research interests include software design patterns and software agents.

Douglas Jones received a PhD in Computer Science from the University of Illinois at Urbana (1980). Currently, he is an Associate Professor of Computer Science at the University of Iowa, and serves as Chair of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems.

Maria Karyda holds an MSc in Information Systems from the Athens University of Economics and Business, where she is a PhD candidate and a member of the Infosec Research Group. Her research interests focus on information systems security policies and management.

Sokratis Katsikas is a Professor of Informatics with the Dept. of Information and Communication Systems Engineering, and the Vice-Rector of the University of the Aegean. He is the Scientific Director of the *e-vote* project (an Internet-based electronic voting system), which is sponsored by the IST Programme of the European Commission.

Aggelos Kiayias holds a PhD and a MA in Computer Science from the City University of New York. His main research area is cryptography and computer security. Dr. Kiayias is a graduate of the Dept. of Mathematics of the University of Athens and a Fulbright Fellow.

Raphaël Kies is a PhD candidate with the Dept. of Political Sciences at the European University Institute, Italy. He graduated in Political Science and is currently working in the field of e-democracy and the public sphere.

Costas Lambrinoudakis holds a PhD in Computer Science from the University of London. He is a Lecturer with the Dept. of Information and Communication Systems Engineering of the University of the Aegean. He is the Technical Director of the *e-vote* project (an Internet-based electronic voting system), which is sponsored by the European Commission. His research interests include secure systems, smart cards, and risk assessment methods.

Emmanouil Magkos is a PhD student with the Dept. of Informatics of Piraeus University, where from he got his BSc on Informatics. His research interests include cryptography and techniques for securing electronic voting, auctions, key escrow, and copyright protection.

Fernando Mendez is a PhD candidate with the Dept. of Political Sciences at the European University Institute, Italy. He holds an MSc in European Politics from the London School of Economics and is conducting research on the United States and the European Union Internet policies.

Rebecca Mercuri holds a PhD from the University of Pennsylvania. She is an Assistant Professor with the Computer Science faculty at Bryn Mawr College. Her research efforts are focused on interactive, real-time systems and digital multimedia. She is the author of a computer security column for *Communications of the ACM.* Her website can be viewed at: http://www.notablesoftware.com/evote.html

Lilian Mitrou holds a PhD in Data Protection from Goethe University of Frankfurt (1992). She is an Assistant Professor of Law with the Dept. of Information and Communication Systems Engineering of the University of the Aegean. She is, also, the Head of the Organization and Administration Directorate of the Office of the Prime Minister of Greece, and an Associate Data Protection Commissioner of Greece.

Peter Neumann holds PhD degrees from Harvard and Darmstadt Universities. He is a Fellow and Principal Scientist at SRI International's Computer Science Laboratory, where he conducts research on computer systems and networks, security, reliability, survivability, safety, and risks-related issues. His book, *Computer-Related Risks*, is in its fifth printing by Addison-Wesley. His website can be viewed at: http://www.csl.sri.com/neumann

Rene Peralta holds a PhD in Computer Science from the University of California at Berkeley. He also studied Economics and Mathematics. He has worked at institutions including the Catholic University of Chile, University of Wisconsin, Amsterdam's Mathematics Center, and Japan's Advanced Institute of Science and Technology. Currently, he is with the Dept of Computer Science of Yale University.

Giusi Poletti holds a PhD in Computer Science (2001). She is a Research Associate with the Dept. of Computer Science of the University of Milan. Her research interests include system security and - in particular - online voting protocols.

Gerald Quirchmayr holds a PhD in Computer Science and Law from Johannes Kepler University. He is a Professor with the Institute for Computer Science and Business Informatics of the University of Vienna. On 1995 he received the IFIP Silver Core Award. His research interests focus on information systems (formal representations of decision-making, security aspects, legal issues).

Emilia Rosti holds a PhD in Computer Science (1993). She is an Associate Professor at the Dept. of Computer Science of the University of Milan, where she teaches operating systems. Her research interests include computer and network security, and computer system performance evaluation.

Gorm Salomonsen holds a PhD in Mathematics (1996). He has held post-doctoral positions at the University of Bonn and at the University of Aarhus. On 1999 he joined Cryptomathic A/S, where he has been working with PKI, electronic voting and other topics.

Roy Saltman, MS, MPA, has worked in the field of election policy and technology for over 25 years. He has served as a consultant to international organizations and vendors of election equipment and software. He is well known for his reports published by the National Institute of Standards and Technology (NIST).

Alexander Trechsel is a graduate in Political Sciences of the University of Geneva, where he took his PhD in 1999. He is the Vice-Director of the Research and Documentation Centre on Direct Democracy (c2d) at the University of Geneva, where he also teaches. His research interests focus on direct democracy and e-democracy.

Vassilis Tsoumas holds an MSc in Information Systems from the Athens University of Economics and Business, where he is a PhD candidate and a member of the Infosec Research Group. His research interests include voting systems, network security, and risk assessment methods.

Moti Yung is the Chief Scientist of CertCo and a visiting faculty at Columbia University. Previously, he was with IBM Research where he received IBM's outstanding innovation award. He is an Editor of the *Journal of Cryptology* and of the *International Journal for Information Security*.

Preface

Elections, referenda and polls are critical processes and tools for the appropriate operation of a modern democracy. Not only do they provide the means for the transfer of power from the citizens to their representatives, but they also support citizen's trust and confidence in government and democracy, provided they are functioning as required and designed.

Although election systems were usually the focus of attention of mainly the politicians and the election officials, the case of Florida (US Presidential election 2000) attracted international attention, especially on how elections are administered. Since then, the capabilities and the limitations of electronic voting systems have come to the center of attention. Electronic election systems are, nowadays and in several countries, under intense scrutiny by policy makers, social scientists, computer and network engineers, and activist groups. The issues are whether more reliable, user-friendly and less costly voting systems should be developed, what are the essential legal and constitutional requirements that should be met and how these systems would stimulate citizen participation in the elections. The discussions on these issues have not reached an end; instead, a long lasting and interesting debate is still ongoing.

Citizen's participation is a major aspect of a democratic system. Nowadays the number of citizens who participate in the elections decreases every year. Because of this, among other reasons lately, there has been a growing interest in online voting or voting over the Internet (electronic voting). Electronic voting is seen as a means to make voting more convenient to the average citizen, thus increasing participation. In the beginning, electronic voting was considered as a simple extension of Internet applications from commerce to government. This approach is, however, incorrect, since election systems must meet certain high standards with regards to security, privacy, etc. Thus, electronic voting is far more challenging, in terms of requirements, than most e-commerce applications. On the other hand, although the democratic process requires and warrants a high level of security, the implemented security measures should not be cumbersome to the voters, otherwise participation may be discouraged.

Recent reports (e.g. CalTech-MIT Report, California Internet Voting Task Force, IPI National Workshop on Internet Voting, European Union IST Projects, etc.) describe the capabilities of e-voting systems, and at the same time identify their limitations, the risks and vulnerabilities they are exposed to, as well as the social concerns such systems give birth to. For example, the possibility of malicious software attacks against computers used for electronic voting cannot be ignored. Such an attack could result in a denial of service, in the submission of software-altered ballots, etc. Some reports argue that despite these challenges, it is technologically feasible to build an electronic voting system that is at least as secure from vote tampering as the current absentee ballot schemes. In any case, most experts in the field agree that an appropriate balance between security, accessibility and ease-of-use must be achieved before an electronic voting system is deployed.

According to recent reports, e-voting systems can be generically grouped into three general categories: Poll, Info-kiosk, and Remote. The means used for their grouping is the location where the ballot is cast. The location leads to the identification of the social concerns and the risks and vulnerabilities, which are associated with each group. Poll voting (e-polling) seems to be more convenient and efficient than traditional voting systems, because the voters can cast their ballots from any location, and the tallying process is fast and valid. Provided that the election officials can control the voting platform and the physical environment, effective management of the inherent security risks seems feasible. In Info-kiosk schemes (i-voting), voting machines are located away from traditional polling places. The i-voting platform and physical installation should be under the control of election officials and should also be appropriately monitored in order to meet security and privacy requirements and to prevent intervention (e.g. coercion). I-voting computers are exposed to more risks than poll systems are.

It is arguable whether all risks and vulnerabilities can be faced with through existing or emerging security technologies. Remote Internet voting (r-voting) provides the voters with convenience and ease-of-access, by enabling them to cast ballots from any Internet accessible location. R-voting offers significant benefits but it also poses substantial security risks and other social concerns. Without official control of the r-voting platform and the physical environment, there are several known ways for one to intervene and alter the election results. Current and emerging technologies seem, for the time being, inadequate to address the inherent risks.

This volume addresses the capabilities and limitations and the trends and perspectives of e-voting technologies, with a particular emphasis on security and privacy issues. It also discusses the feasibility of the different forms of electronic voting, from both the technical and social science perspectives. Finally, it discusses whether electronic voting is to be viable in the foreseeable future, and - if yes - under what conditions.

The volume is divided into three parts. The first part introduces the reader to the current electronic voting scene. The second part refers to the trends and perspectives in this field, worldwide. Finally, the third part provides the reader with state-of-the-art research results, focusing on the capabilities and limitations of the existing and emerging electronic voting technologies.

Part I addresses the current status in the electronic voting arena. It includes four papers, and its aim is twofold; first, to provide the reader with an extensive introduction to the emerging electronic voting scene; second, to describe the generic requirements for the electronic voting systems. *Jones* provides an evaluation of the existing voting technologies, considering them as part of a larger social and legal system. *Cranor* discusses the search of the perfect voting technology. After a thorough analysis, she argues that there might be partial answers to this problem but an appropriate solution is still pending. *Mercuri and Neumann*, after referring to the risks that pertain to system design, misuse, and sociological factors, describe the difficulties in validating fully computerized election equipment, and express their concerns for Internet-based systems. *Mitrou, Gritzalis, Katsikas and Quirchmayr* review the legal and constitutional needs, and identify and describe the reflecting technical requirements that a voting system should comply with.

Part II refers to the trends and perspectives in the electronic voting world. It includes three papers, which address existing and emerging methodologies for the development of secure electronic voting systems. *Burmester and Magkos* overview the main electronic voting schemes, assess their security and practicality, analyze the security risks and discuss methods to minimize them. *Damgård, Groth and Salomonsen* describe the theory and discuss various issues regarding the security of an online voting scheme, based on homomorphic encryption. *Lambrinoudakis, Gritzalis, Tsoumas, Karyda and Ikonomopoulos*, after presenting the security requirements and the system-wide properties that an electronic voting system is expected to fulfill, provide an overview of the existing voting protocols and a brief analysis of their characteristics.

Part III includes seven papers; it addresses electronic voting systems capabilities and limitations, and provides the reader with a series of answers on how to cope with the issues appearing during the development of secure electronic voting systems. *Saltman* discusses the auditability and voter confidence issues in direct-recording voting systems. *Kiayias and Yung* present a robust verifiable non-interactive zero-sharing voting utility, which enables a set of voters to protect the privacy of their votes, even in settings where all authorities may be dishonest and try to violate a voter's privacy. *Peralta* provides the readers with arguments for and against deploying electronic voting technology; he concludes that a multidisciplinary effort is essential to build, deploy, and evaluate the new technology. *Gerck* describes the Distributed Voting System, an Internet voting system using mesh networks to implement a protocol offering privacy, security and auditing, with receipt-freeness and universal verifiability. *Treschel, Mendez and Kies* describe and discuss - from a social scientist's point of view - the Canton of Geneva (Switzerland) pilot project on remote voting via the Internet. Digital divide, desirability and user friendliness are issues, which are discussed and comment upon. *Bruschi, Poletti and Rosti* describe how a Public Key Infrastructure may be used in electronic voting, with an eye towards performance issues and in particular in the case of disaster recovery. The book concludes with a paper authored by *Chaum*, which focuses on untraceable electronic mail, return addresses, and digital pseudonyms; the paper appeared for the first time (in *Com. of the ACM*) more than 20 years ago and it is considered a breakthrough in the field.

In summary, the volume provides researchers, legal experts, public policy makers, and practitioners with an in-depth review on secure electronic voting trends and perspectives, capabilities and limitations. In particular, practitioners, researchers, and legal experts can benefit from the data protection and privacy papers, in addition to the state-of-the-art research results, which are also described and commented upon. Public policy makers, election organizers and social scientists can gain insight from the analysis of the socio-technical context of the electronic voting systems and technologies.

Several distinguished experts in the field of IT security or electronic voting accepted my invitation and prepared valuable contributions. Kluwer Academic Publishers accepted my proposal and gave me the opportunity to serve as the editor of this volume. S. Lagerstrom-Fife - my publishing editor - was always ready to help, when I needed her advice and guidance. S. Jajodia, the Consulting Editor of the *Advances in Information Security* Series, offered me his generous encouragement and continuous support. My wife and our daughters provided me with their strongest support and understanding - as always. Thank you all, folks!

Dimitris A. Gritzalis (dgrit@aueb.gr)
Dept. of Informatics
Athens University of Economics and Business
Athens, Greece