Sabrina De Capitani di Vimercati
Paul Syverson
Dieter Gollmann (Eds.)

LNCS 3679

Computer Security – ESORICS 2005

10th European Symposium on Research in Computer Security
Milan, Italy, September 2005
Proceedings

Sabrina De Capitani di Vimercati
Paul Syverson Dieter Gollmann (Eds.)

Computer Security – ESORICS 2005

10th European Symposium on Research in Computer Security
Milan, Italy, September 12-14, 2005
Proceedings

Springer

Volume Editors

Sabrina De Capitani di Vimercati
Universitá degli Studi di Milano
Dipartimento di Tenologie dell'Informazione
Via Bramante 65, 26013 Crema (CR), Italy
E-mail: decapita@dti.unimi.it

Paul Syverson
Naval Research Laboratory Washington
Center for High Assurance Computer Systems
Washington DC 20375, USA
E-mail: syverson@itd.nrl.navy.mil

Dieter Gollmann
TU Hamburg-Harburg, 21071 Hamburg, Germany
E-mail: diego@tu-harburg.de

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.5, C.2.0, H.2.0, K.6.5, K.4.4

ISSN 0302-9743
ISBN-10 3-540-28963-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28963-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11555827 06/3142 5 4 3 2 1 0

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

Foreword from the Program Chairs

These proceedings contain the papers selected for presentation at the 10th European Symposium on Research in Computer Security (ESORICS), held September 12–14, 2005 in Milan, Italy.

In response to the call for papers 159 papers were submitted to the conference. These papers were evaluated on the basis of their significance, 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 submitted, 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 Publicity 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 find the program stimulating.

July 2005 Sabrina De Capitani di Vimercati and Paul Syverson

Foreword from the General Chair

It is my pleasure to welcome you to the 10th European Symposium On Research In Computer Security in Milan. Initially established as the European conference in research on computer security, ESORICS has reached the status of a main international event gathering researchers from all over the world. The conference, hosted for the first time in Milan, offers an outstanding technical program, including one invited talk and 27 selected papers.

An event like this does not just happen; it depends on the volunteer efforts of a host of individuals. I wish to express my sincere appreciation to all the people who volunteered their time and energy to put together the conference and make it possible. First and foremost, thanks are due to Sabrina De Capitani di Vimercati and Paul Syverson and the members of the program committee for selecting the technical papers for presentation and to Barbara Simons for agreeing to deliver the keynote speech. I am also grateful to all those people who ensured a smooth organization process: Dieter Gollmann, for collating the proceedings volume and ensuring that these proceedings be ready for distribution at the conference; Claudio Ardagna for serving as Publicity Chair; Emilia Rosti for helping with the organization and taking care of local arrangements; and Olga Scotti for her help with local arrangements.

Special thanks are due to: the University of Milan, for granting us the conference location and service; the Department of Information Technologies of the University for its support; the Italian Association for Information Processing (AICA) for its financial support and for providing help in the secretarial and registration process; and the sponsors for their support.

Last, but certainly not least, thanks to all of you for attending the conference. I hope you find the program stimulating and enjoy your time in Milan!

Pierangela Samarati

Organization

Program Committee

Rakesh Agrawal	IBM Almaden Research Center, USA
Gerard Allwein	Naval Research Laboratory, USA
Ross Anderson	University of Cambridge, UK
Vijay Atluri	Rutgers University, USA
Michael Backes	IBM Zurich Research Laboratory, Switzerland
Giampaolo Bella	University of Catania, Italy
Jan Camenisch	IBM Zurich Research Laboratory, Switzerland
David Chadwick	University of Kent, UK
LiWu Chang	Naval Research Laboratory, USA
Marc Dacier	Institut Eurécom, France
Ernesto Damiani	Università degli Studi di Milano, Italy
George Danezis	University of Cambridge, UK
Sabrina De Capitani di Vimercati (co-chair)	Università degli Studi di Milano, Italy
Simon Foley	University College Cork, Ireland
Philippe Golle	Palo Alto Research Center, USA
Marit Hansen	ICPP Schleswig-Holstein, Germany
Philippa Hopcroft	Oxford University, UK
Sushil Jajodia	George Mason University, USA
Dogan Kesdogan	RWTH Aachen, Informatik IV, Germany
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Patrick McDaniel	Pennsylvania State University, USA
Heiko Mantel	ETH-Zentrum, Switzerland
Nick Mathewson	The Free Haven Project, USA
Richard E. Newman	University of Florida, USA
Peng Ning	NC State University, USA
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Emilia Rosti	Università degli Studi di Milano, Italy
Peter Ryan	University of Newcastle upon Tyne, UK
Kazue Sako	NEC Corporation, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Paul Syverson (co-chair)	Naval Research Laboratory, USA
Vanessa Teague	University of Melbourne, Australia
Brent Waters	Stanford University, USA
Mariemma I. Yagüe	University of Malaga, Spain
Alec Yasinsac	Florida State University, USA
Sheng Zhong	State University of New York at Buffalo, USA

Additional Reviewers

Todd Andel,
Ben Aziz
Walid Bagga
Sebastiano Battiato
Birgit Baum-Waidner
Meletis Belsis
Peter Berlich
Mike Bond
Kevin Butler
Achim Brucker
Jeremy Bryans
Christian Cachin
Shiping Chen
Shu-Ching Chen
Yannick Chevalier
Richard Clayton
Andrew Conway
Amy Corman
Lavinia Egidi
Will Enck
Jun Furukawa
Michael Goldsmith
Steven Greenwald
Qijun Gu
Huiping Guo
Markus Hansen
Shan He
Boniface Patrick Hicks
Martin Hirt
Dennis Hofheinz
Susan Hohenberger
Toshinori Araki
Toshiyuki Isshiki
Tobias Kölsch
Kameswari Kotapati
Fengjun Li
Huiyun Li
Lunquan Li
Jay Ligatti
Anyi Liu
Donggang Liu
Wesam Lootah
Gavin Lowe
Ashwin Machanavajjhala
Todd McDonald
Martin Meints
Jose A. Montenegro
Kengo Mori
Barry Mulcahy
Gregory Neven
Tom Newcomb
Satoshi Obana
Jose A. Onieva
Joseph Pamula
Chi-Chun Pan
Udaya Parampalli
Thea Peacock
Alexis Pimenidis
Fabien Pouget
Thomas Probst
Ahmad-Reza Sadeghi
Ralf Rantzau
Arnon Rosenthal
Sankardas Roy
Patrizia Scandurra
Tim Seipold
Christos Siaterlis
Barbara Sprick
Rainer Steinwandt
Isamu Teranishi
Patrick Traynor
Ingrid Verbauwhede
Frederik Vercauteren
Ulrich Waldmann
Hai Wang
Lingyu Wang
Xinyuan Wang
Bogdan Warinschi
Ralf Wienzek
Duminda Wijesekera
Min Wu
Dingbang Xu
Jun Xu
Meng Yu
Stefano Zanero
Justin Zhan
Lei Zhang
Hongbin Zhou

Lecture Notes in Computer Science

For information about Vols. 1–3598

please contact your bookseller or Springer

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3718: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XII, 502 pages. 2005.

Vol. 3714: H. Obbink, K. Pohl (Eds.), Software Product Lines. XIII, 235 pages. 2005.

Vol. 3710: M. Barni, I. Cox, T. Kalker, H.J. Kim (Eds.), Digital Watermarking. XII, 485 pages. 2005.

Vol. 3703: F. Fages, S. Soliman (Eds.), Principles and Practice of Semantic Web Reasoning. VIII, 163 pages. 2005.

Vol. 3702: B. Beckert (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. XIII, 343 pages. 2005. (Subseries LNAI).

Vol. 3698: U. Furbach (Ed.), KI 2005: Advances in Artificial Intelligence. XIII, 409 pages. 2005. (Subseries LNAI).

Vol. 3697: W. Duch, J. Kacprzyk, E. Oja, S. Zadrożny (Eds.), Artificial Neural Networks: Formal Models and Their Applications - ICANN 2005, Part II. XXXII, 1045 pages. 2005.

Vol. 3696: W. Duch, J. Kacprzyk, E. Oja, S. Zadrożny (Eds.), Artificial Neural Networks: Biological Inspirations - ICANN 2005, Part I. XXXI, 703 pages. 2005.

Vol. 3691: A. Gagalowicz, W. Philips (Eds.), Computer Analysis of Images and Patterns. XIX, 865 pages. 2005. (Subseries LNAI).

Vol. 3690: M. Pěchouček, P. Petta, L.Z. Varga (Eds.), Multi-Agent Systems and Applications IV. XVII, 667 pages. 2005. (Subseries LNAI).

Vol. 3687: S. Singh, M. Singh, C. Apte, P. Perner (Eds.), Pattern Recognition and Image Analysis, Part II. XXV, 809 pages. 2005.

Vol. 3686: S. Singh, M. Singh, C. Apte, P. Perner (Eds.), Pattern Recognition and Data Mining, Part I. XXVI, 689 pages. 2005.

Vol. 3684: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part IV. LXXIX, 933 pages. 2005. (Subseries LNAI).

Vol. 3683: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. LXXX, 1397 pages. 2005. (Subseries LNAI).

Vol. 3682: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. LXXIX, 1371 pages. 2005. (Subseries LNAI).

Vol. 3681: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXXX, 1319 pages. 2005. (Subseries LNAI).

Vol. 3679: S.De Capitani di Vimercati, P. Syverson, D. Gollmann (Eds.), Computer Security – ESORICS 2005. XI, 509 pages. 2005.

Vol. 3678: A. McLysaght, D.H. Huson (Eds.), Comparative Genomics. VIII, 167 pages. 2005. (Subseries LNBI).

Vol. 3677: J. Dittmann, S. Katzenbeisser, A. Uhl (Eds.), Communications and Multimedia Security. XIII, 360 pages. 2005.

Vol. 3675: Y. Luo (Ed.), Cooperative Design, Visualization, and Engineering. XI, 264 pages. 2005.

Vol. 3674: W. Jonker, M. Petković (Eds.), Secure Data Management. X, 241 pages. 2005.

Vol. 3672: C. Hankin, I. Siveroni (Eds.), Static Analysis. X, 369 pages. 2005.

Vol. 3671: S. Bressan, S. Ceri, E. Hunt, Z.G. Ives, Z. Bellahsène, M. Rys, R. Unland (Eds.), Database and XML Technologies. X, 239 pages. 2005.

Vol. 3670: M. Bravetti, L. Kloul, G. Zavattaro (Eds.), Formal Techniques for Computer Systems and Business Processes. XIII, 349 pages. 2005.

Vol. 3665: K. S. Candan, A. Celentano (Eds.), Advances in Multimedia Information Systems. X, 221 pages. 2005.

Vol. 3664: C. Türker, M. Agosti, H.-J. Schek (Eds.), Peer-to-Peer, Grid, and Service-Orientation in Digital Library Architectures. X, 261 pages. 2005.

Vol. 3663: W.G. Kropatsch, R. Sablatnig, A. Hanbury (Eds.), Pattern Recognition. XIV, 512 pages. 2005.

Vol. 3662: C. Baral, G. Greco, N. Leone, G. Terracina (Eds.), Logic Programming and Nonmonotonic Reasoning. XIII, 454 pages. 2005. (Subseries LNAI).

Vol. 3661: T. Panayiotopoulos, J. Gratch, R. Aylett, D. Ballin, P. Olivier, T. Rist (Eds.), Intelligent Virtual Agents. XIII, 506 pages. 2005. (Subseries LNAI).

Vol. 3660: M. Beigl, S. Intille, J. Rekimoto, H. Tokuda (Eds.), UbiComp 2005: Ubiquitous Computing. XVII, 394 pages. 2005.

Vol. 3659: J.R. Rao, B. Sunar (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2005. XIV, 458 pages. 2005.

Vol. 3658: V. Matoušek, P. Mautner, T. Pavelka (Eds.), Text, Speech and Dialogue. XV, 460 pages. 2005. (Subseries LNAI).

Vol. 3655: A. Aldini, R. Gorrieri, F. Martinelli (Eds.), Foundations of Security Analysis and Design III. VII, 273 pages. 2005.

Vol. 3654: S. Jajodia, D. Wijesekera (Eds.), Data and Applications Security XIX. X, 353 pages. 2005.

Vol. 3653: M. Abadi, L. de Alfaro (Eds.), CONCUR 2005 – Concurrency Theory. XIV, 578 pages. 2005.

Vol. 3652: A. Rauber, S. Christodoulakis, A M. Tjoa (Eds.), Research and Advanced Technology for Digital Libraries. XVIII, 545 pages. 2005.

Vol. 3649: W.M.P. van der Aalst, B. Benatallah, F. Casati, F. Curbera (Eds.), Business Process Management. XII, 472 pages. 2005.

Vol. 3648: J.C. Cunha, P.D. Medeiros (Eds.), Euro-Par 2005 Parallel Processing. XXXVI, 1299 pages. 2005.

Vol. 3646: A. F. Famili, J.N. Kok, J.M. Peña, A. Siebes, A. Feelders (Eds.), Advances in Intelligent Data Analysis VI. XIV, 522 pages. 2005.

Vol. 3645: D.-S. Huang, X.-P. Zhang, G.-B. Huang (Eds.), Advances in Intelligent Computing, Part II. XIII, 1010 pages. 2005.

Vol. 3644: D.-S. Huang, X.-P. Zhang, G.-B. Huang (Eds.), Advances in Intelligent Computing, Part I. XXVII, 1101 pages. 2005.

Vol. 3642: D. Ślezak, J. Yao, J.F. Peters, W. Ziarko, X. Hu (Eds.), Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing, Part II. XXIII, 738 pages. 2005. (Subseries LNAI).

Vol. 3641: D. Ślezak, G. Wang, M. Szczuka, I. Düntsch, Y. Yao (Eds.), Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing, Part I. XXIV, 742 pages. 2005. (Subseries LNAI).

Vol. 3639: P. Godefroid (Ed.), Model Checking Software. XI, 289 pages. 2005.

Vol. 3638: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), Smart Graphics. XI, 269 pages. 2005.

Vol. 3637: J. M. Moreno, J. Madrenas, J. Cosp (Eds.), Evolvable Systems: From Biology to Hardware. XI, 227 pages. 2005.

Vol. 3636: M.J. Blesa, C. Blum, A. Roli, M. Sampels (Eds.), Hybrid Metaheuristics. XII, 155 pages. 2005.

Vol. 3634: L. Ong (Ed.), Computer Science Logic. XI, 567 pages. 2005.

Vol. 3633: C. Bauzer Medeiros, M. Egenhofer, E. Bertino (Eds.), Advances in Spatial and Temporal Databases. XIII, 433 pages. 2005.

Vol. 3632: R. Nieuwenhuis (Ed.), Automated Deduction – CADE-20. XIII, 459 pages. 2005. (Subseries LNAI).

Vol. 3631: J. Eder, H.-M. Haav, A. Kalja, J. Penjam (Eds.), Advances in Databases and Information Systems. XIII, 393 pages. 2005.

Vol. 3630: M.S. Capcarrere, A.A. Freitas, P.J. Bentley, C.G. Johnson, J. Timmis (Eds.), Advances in Artificial Life. XIX, 949 pages. 2005. (Subseries LNAI).

Vol. 3629: J.L. Fiadeiro, N. Harman, M. Roggenbach, J. Rutten (Eds.), Algebra and Coalgebra in Computer Science. XI, 457 pages. 2005.

Vol. 3628: T. Gschwind, U. Aßmann, O. Nierstrasz (Eds.), Software Composition. X, 199 pages. 2005.

Vol. 3627: C. Jacob, M.L. Pilat, P.J. Bentley, J. Timmis (Eds.), Artificial Immune Systems. XII, 500 pages. 2005.

Vol. 3626: B. Ganter, G. Stumme, R. Wille (Eds.), Formal Concept Analysis. X, 349 pages. 2005. (Subseries LNAI).

Vol. 3625: S. Kramer, B. Pfahringer (Eds.), Inductive Logic Programming. XIII, 427 pages. 2005. (Subseries LNAI).

Vol. 3624: C. Chekuri, K. Jansen, J.D.P. Rolim, L. Trevisan (Eds.), Approximation, Randomization and Combinatorial Optimization. XI, 495 pages. 2005.

Vol. 3623: M. Liśkiewicz, R. Reischuk (Eds.), Fundamentals of Computation Theory. XV, 576 pages. 2005.

Vol. 3622: V. Vene, T. Uustalu (Eds.), Advanced Functional Programming. IX, 359 pages. 2005.

Vol. 3621: V. Shoup (Ed.), Advances in Cryptology – CRYPTO 2005. XI, 568 pages. 2005.

Vol. 3620: H. Muñoz-Avila, F. Ricci (Eds.), Case-Based Reasoning Research and Development. XV, 654 pages. 2005. (Subseries LNAI).

Vol. 3619: X. Lu, W. Zhao (Eds.), Networking and Mobile Computing. XXIV, 1299 pages. 2005.

Vol. 3618: J. Jedrzejowicz, A. Szepietowski (Eds.), Mathematical Foundations of Computer Science 2005. XVI, 814 pages. 2005.

Vol. 3617: F. Roli, S. Vitulano (Eds.), Image Analysis and Processing – ICIAP 2005. XXIV, 1219 pages. 2005.

Vol. 3615: B. Ludäscher, L. Raschid (Eds.), Data Integration in the Life Sciences. XII, 344 pages. 2005. (Subseries LNBI).

Vol. 3614: L. Wang, Y. Jin (Eds.), Fuzzy Systems and Knowledge Discovery, Part II. XLI, 1314 pages. 2005. (Subseries LNAI).

Vol. 3613: L. Wang, Y. Jin (Eds.), Fuzzy Systems and Knowledge Discovery, Part I. XLI, 1334 pages. 2005. (Subseries LNAI).

Vol. 3612: L. Wang, K. Chen, Y. S. Ong (Eds.), Advances in Natural Computation, Part III. LXI, 1326 pages. 2005.

Vol. 3611: L. Wang, K. Chen, Y. S. Ong (Eds.), Advances in Natural Computation, Part II. LXI, 1292 pages. 2005.

Vol. 3610: L. Wang, K. Chen, Y. S. Ong (Eds.), Advances in Natural Computation, Part I. LXI, 1302 pages. 2005.

Vol. 3608: F. Dehne, A. López-Ortiz, J.-R. Sack (Eds.), Algorithms and Data Structures. XIV, 446 pages. 2005.

Vol. 3607: J.-D. Zucker, L. Saitta (Eds.), Abstraction, Reformulation and Approximation. XII, 376 pages. 2005. (Subseries LNAI).

Vol. 3606: V. Malyshkin (Ed.), Parallel Computing Technologies. XII, 470 pages. 2005.

Vol. 3605: Z. Wu, M. Guo, C. Chen, J. Bu (Eds.), Embedded Software and Systems. XIX, 610 pages. 2005.

Vol. 3604: R. Martin, H. Bez, M. Sabin (Eds.), Mathematics of Surfaces XI. IX, 473 pages. 2005.

Vol. 3603: J. Hurd, T. Melham (Eds.), Theorem Proving in Higher Order Logics. IX, 409 pages. 2005.

Vol. 3602: R. Eigenmann, Z. Li, S.P. Midkiff (Eds.), Languages and Compilers for High Performance Computing. IX, 486 pages. 2005.

Vol. 3599: U. Aßmann, M. Aksit, A. Rensink (Eds.), Model Driven Architecture. X, 235 pages. 2005.

Table of Contents

Computerized Voting Machines: A View from the Trenches

Barbara Simons

simons@acm.org

As a result of Florida 2000, some Americans concluded that paper ballots simply couldn't be counted, even though businesses, banks, racetracks, lottery systems, and others count and deal with paper all the time. Instead, paperless computerized voting systems (Direct Recording Electronic or DREs) were touted as the solution to "the Florida problem".

Election officials in the U.S. were told that DREs in the long run would be cheaper than alternative voting systems. They also were told that DREs had been extensively tested and that the certification process guaranteed that the machines were reliable and secure. No mention was made of the costs ballot design, of pre-election testing, and of secure storage of DREs; nothing was said about the threat of hidden malicious code; no mention was made of the inadequacy of the testing and certification processes, to say nothing of the difficulty of creating bug-free software.

Why were independent computer security experts not consulted about such a major and fundamental change in how elections are held? Why were some election officials and policy makers hostile when computer security experts warned of the risks of computerized voting to the point of accusing computer scientists of being "fear mongers" and Luddites? How could Harris Miller, the President of the Information Technology Association of America, a lobbying organization that has received compensation from voting machine vendors, claim on Election Day 2004 that, "Electronic voting machine issues that have been cited are related to human error, process missteps or unsubstantiated reports"? How would he know? Why would anyone listen to him?

Why do many election officials and politicians believe that internet voting would increase voter turnout in the U.S., even though no rigorous testing has occurred? And, even if internet voting would increase turnout, how can these same people who have been reading about internet viruses for years not understand that internet voting is a very very risky proposition?

In short, why have DRE vendors and many election officials succeeded at challenging the expertise of computer scientists and computer security experts?

The refusal of policy makers to listen to the computing community hardly began with the introduction of poorly engineered and insecure voting machines. Many computer scientists and computer security experts became involved with policy debates over crypto policy, copyright, patents, and computerized surveillance – to name some of the major issues.

The disconnect between the computing community and policy makers is perhaps best illustrated by the Digital Millennium Copyright Act (DMCA),

S. De Capitani di Vimercati et al. (Eds.): ESORICS 2005, LNCS 3679, pp. 1–2, 2005.

which became part of US law in 1998. It was only by chance that I learned why implementation of the most controversial aspects of the DMCA, the anti-circumvention and anti-dissemination provisions, was postponed until 2000. The delay was written into the DMCA because lawmakers knew, or someone they trusted told them, that aspects of the DMCA might criminalize work on securing software against Y2K problems. Yet, the fact that Y2K was hardly the only software security issue that would require the kinds of reverse engineering that was done to fix Y2K bugs was either unknown to the lawmakers or a matter of indifference to them.

A discussion of the DMCA brings us full circle back to the issue of computerized voting systems. In the U.S. the software that is deployed in these systems is secret, as is the testing – paid for by the software vendors – and the test results. Because of the anti-circumvention provisions of the DMCA, computer security experts risk violating U.S. Federal law if they wish to reverse engineer voting machine software to search for bugs or malicious code. Consequently, a law that was crafted by the movie and record industries to prevent unauthorized copying is assisting voting machine vendors with concealing their software from meaningful independent review.

Clearly, we computing professionals have been failing at explaining the risks of inappropriate, careless, or poorly designed software to the general public and especially to policy makers, at least in the U.S. (At this conference I hope to learn more about what is happening in Europe). While perhaps not enough of us have become involved with efforts to educate policy makers, there are some fundamental reasons why our expertise is frequently ignored:

1. People who have never done much programming do not understand how difficult it is to find bugs in software.
2. Because people don't understand point 1, they certainly don't understand that last minute software patches are very dangerous.
3. Consequently, most people have a hard time believing computer security experts when they say that it's possible to write malicious code and conceal it in a large program. They just don't understand why it can be very difficult to determine that malware is present, let alone locate it in a large body of code.

In addition, we are a relatively young profession, and many of us have an independent streak and a casual mode of dress that, taken together, make some politicians view us as potential trouble makers, rather than as people whose views the politicians should take seriously.

Yet, we must make our voices heard. The issues are too critical to allow us to be shut out of the debate.

I'll give an overview of some of the technological and policy issues relating to computerized voting machines, and perhaps touch on how we might do a better job of getting our message across. I also look forward to hearing ideas that others might have of how we might better explain software-related risks to non-technical decision makers.

XML Access Control with Policy Matching Tree

Naizhen Qi (Naishin Seki) and Michiharu Kudo

IBM Research, Tokyo Research Laboratory,
1623-14, Shimo-tsuruma, Yamato-shi,
Kanagawa 242-8502, Japan
{naishin, kudo}@jp.ibm.com

Abstract. XML documents are frequently used in applications such as business transactions and medical records involving sensitive information. Access control on the basis of data location or value in an XML document is therefore essential. However, current approaches to efficient access control over XML documents have suffered from scalability problems because they tend to work on individual documents. To resolve this problem, we proposed a table-based approach in [28]. However, [28] also imposed limitations on the expressiveness, and real-time access control updates were not supported. In this paper, we propose a novel approach to XML access control through a policy matching tree (PMT) which performs accessibility checks with an efficient matching algorithm, and is shared by all documents of the same document type. The expressiveness can be expanded and real-time updates are supported because of the PTM's flexible structure. Using synthetic and real data, we evaluate the performance and scalability to show it is efficient for checking accessibility for XML databases.

1 Introduction

XML [7] data is becoming more prevalent as more businesses and systems become integrated over the Web. In applications such as business transactions and medical records, sensitive data may be scattered throughout an XML document and access control at the node level (element or attribute) is required to ensure that sensitive data can only be accessed by authorized users. Access control must be expressive and be able to support rules that select data based on the location and value(s) of the data. In practice, the number of access control rules can be on the order of millions, which is a product of the number of document types (in 1,000's) and the number of user roles (in 100's). Therefore, the solution also requires high scalability and performance.

Several XML access control models [4,11,17,23] provide expressive access control over XML documents. These approaches usually support grant or denial access control specifications, a propagation mechanism whereby descendant elements inherit rules from their parents, and conflict resolution in case the data is covered by multiple access control rules. Since these models perform access control by traversing XML documents at runtime, the enforcement imposes heavy

S. De Capitani di Vimercati et al. (Eds.): ESORICS 2005, LNCS 3679, pp. 3–23, 2005.

computational costs especially for deeply layered XML documents with large and expressive access control rules.

Ideas to efficiently provide expressive access control have been proposed in [3,9,12,28,30]. These approaches are effective in efficiently searching for access controlled nodes [3,12,30], or in eliminating unnecessary accessibility checks at runtime [9]. These research efforts have managed to improve the efficiency of expressive access control. However, since they generally focus on document-based optimizations, XML databases with frequent updates of either the documents or access control rules may incur unacceptable costs. In our previous research [28], we proposed an efficient table-driven access control model that takes into account XML document updates. It provides runtime efficiency but has limitations on access control expressiveness and the real-time update of access control rules was not supported.

In this paper, we develop an effifffcient and expressive access control model applicable to existing access control models [4,11,23] for XML documents. The novelties of this access control model are a data-independent optimization so that XML data updates will not trigger any recomputations, and that real-time policy update is supported. The key idea is to build a policy matching tree, a PMT, on the basis of the access control rules. The accessibility check is performed by matching the access request against the PMT and deciding on the basis of the matching results. Since all of the rules in the PMT are isolated from each other, the PMT is capable of handling real-time PMT updates. An accessibility cache improves runtime performance by skipping duplicated accessibility evaluations on the same paths. Through experiments, we show the PMT is capable of supporting millions of access control rules efficiently.

The rest of this paper is organized as follows. After reviewing the concerned access control model in Section 2, we present our solution, the PMT model in Section 3. In Section 4 we describe how to match an access request against the PMT for an accessibility decision. Section 5 describes the access control system on the basis of the PMT. Experimental results are reported in Section 6 and in Section 7 we summarize our conclusions and consider future work.

1.1 Related Work

Many approaches for enforcing XML access control have been proposed. Some of them [17,23] support full [10] expressions to provide expressiveness with straightforward implementations by creating the projection of the access control policy on a DOM [19] tree. However, these approaches incur massive runtime costs when handling a large access control policy or a deeply layered XML document. The mechanisms proposed in [2,4,11,12] perform more efficiently but also encounter the same problem at runtime since node-level access control on a DOM-based view can be expensive when processing large numbers of XML documents.

To overcome this problem, several efficient access control models have been proposed [25,28]. Qi et al. [28], our previous research, presents a method that performs in near-constant time regardless of the number of access control rules. This is achieved by using an access condition table generated from the access control