Lecture Notes in Computer Science 2433

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer-Verlag Berlin Heidelberg GmbH

Agnes Hui Chan Virgil Gligor (Eds.)

Information Security

5th International Conference, ISC 2002
Sao Paulo, Brazil, September 30 - October 2, 2002
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Agnes Hui Chan
College of Computer Science, Northeastern University
Boston, MA 02115, USA
E-mail: ahchan@ccs.neu.edu

Virgil Gligor
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742, USA
E-mail: gligor@eng.umd.edu

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : 5th international conference ; proceedings / ISC 2002, Sao Paulo, Brazil, September 30 - October 2, 2002. Agnes Hui Chan ; Virgil Gligor (ed.).

(Lecture notes in computer science ; Vol. 2433)
ISBN 978-3-540-44270-7

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3

ISSN 0302-9743
ISBN 978-3-540-44270-7 ISBN 978-3-540-45811-1 (eBook)
DOI 10.1007/978-3-540-45811-1

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from
Springer-Verlag Berlin Heidelberg GmbH
Violations are liable for prosecution under the German Copyright Law.

http://www.springer.de

© Springer-Verlag Berlin Heidelberg 2002

Originally published by Springer-Verlag Berlin Heidelberg New York in 2002

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e.K.
Printed on acid-free paper SPIN: 10870122 06/3142 5 4 3 2 1 0

Preface

As distinct from other security and cryptography conferences, the Information Security Conference (ISC) 2002 brought together individuals involved in a wide variety of different disciplines of information security to foster the exchange of ideas. The conference is an outgrowth of the Information Security Workshop, first held in Ishikawa, Japan 1997. ISC 2002 was held in Sao Paulo, Brazil, on September 30–October 2, 2002.

The Program Committee considered 81 submissions of which 38 papers were accepted for presentation. These proceedings contain revised versions of the accepted papers. The papers provide a representative sample of both the variety and the truly international scope of information security research conducted currently. The topics addressed range from e-commerce protocols to access control and trust management, and to cryptography and cryptographic algorithms.

Many people deserve our gratitude for their contribution to the success of the conference. We would like to thank the General Chair, Routo Terada, for overseeing the local arrangements, including registration and maintaining the conference website, and for the smooth running of the conference. We are grateful to Robbie Ye for his expert help in processing the electronic submissions, reviews and acceptance notifications. Robbie's enthusiasm and energy greatly simplified the Program Committee's task of conducting the on-line evaluation of the submitted papers under tight time constraints.

In evaluating the papers submitted we were fortunate to receive the help of a distinguished Program Committee. We wish to thank the committee for doing an excellent job in reviewing papers and providing useful feedback to authors. In addition to the advice of the Program Committee, we also benefited from the expert help of external reviewers, including our colleagues: Jaouhar Ayadi; Dirk Balfanz, Rakesh Bobba, Dan Boneh, M. Cassassa-Mont, C.I. Dalton, Anand Desai, Glenn Durfee, Laurent Eschenauer, David Goldberg, Guang Gong, Anwar Hasan, Hector Ho-Fuentes, Adrian Kent, H. Khurana, R. Koleva, Thiago C. Martins, Muriel Medard, Brian Monahan, Narendar, Mads Rasmussen, Joe Rushanan, David Soldera, Routo Terada, Duncan Wong, Min Wu, Robbie Ye, Muxiang Zhang, and Feng Zhu.

Most of all, we thank all the authors who submitted papers to this conference. Without their submissions, this conference could not have been a success.

July 2002

Agnes Hui Chan
Virgil Gligor

Information Security Conference 2002

September 30 – October 2, 2002, Sao Paulo, Brazil

Conference Chair

Routo Terada, University of Sao Paulo (Brazil)

Program Co-chair

Agnes Hui Chan, Northeastern University (USA)
Virgil D. Gligor, University of Maryland – College Park (USA)

Program Committee

Yolanta Beres ..... HP Labs (UK)
Ricardo Dahab ..... University of Campinas (Brazil)
Drew Dean ..... SRI (USA)
Yair Frankel ..... TechTegrity (USA)
Peter Gutmann ..... University of Auckland (NZ)
John Ioannidis ..... AT&T Labs – Research (USA)
Charlie Kaufman ..... Iris Assoc (USA)
Jay Lala ..... DARPA (USA)
Carl Landwehr ..... NSF (USA)
Teresa Lunt ..... PARC (USA)
Doug Maughan ..... DARPA (USA)
Gary McGraw ..... Cigital (USA)
Cathy Meadows ..... NRL (USA)
Rebecca Mercuri ..... Bryn Mawr College (USA)
Radia Perlman ..... Sun Microsystems (USA)
Radha Poovendran ..... University of Washington (USA)
Gang Qu ..... University of Maryland (USA)
Greg Rose ..... Qualcomm (Australia)
Jonathan Trostle ..... CISCO (USA)

Table of Contents

Intrusion Detection and Tamper Resistance

Real-Time Intruder Tracing through Self-Replication 1
Heejin Jang, Sangwook Kim

On the Difficulty of Protecting Private Keys in Software 17
Taekyoung Kwon

Intrusion Detection with Support Vector Machines and Generative Models 32
John S. Baras, Maben Rabi

Cryptographic Algorithm and Attack Implementation

Small and High-Speed Hardware Architectures for the 3GPP Standard Cipher KASUMI 48
Akashi Satoh, Sumio Morioka

Fast Software Implementations of SC2000 63
Helger Lipmaa

Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512 75
Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen, Peter Bellows, Jaroslav Flidr, Tom Lehman, Brian Schott

Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG . . 90
Kahil Jallad, Jonathan Katz, Bruce Schneier

Access Control and Trust Management (I)

Role-Based Access Control for E-commerce Sea-of-Data Applications 102
G. Navarro, S. Robles, J. Borrell

An Access Control Model for Tree Data Structures 117
Alban Gabillon, Manuel Munier, Jean-Jacques Bascou, Laurent Gallon, Emmanuel Bruno

A New Design of Privilege Management Infrastructure for Organizations Using Outsourced PKI 136
Ed Dawson, Javier Lopez, Jose A. Montenegro, Eiji Okamoto

Authentication and Privacy

Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks 150
Feng Zhu, Duncan S. Wong, Agnes H. Chan, Robbie Ye

Quantifying Privacy Leakage through Answering Database Queries 162
Tsan-sheng Hsu, Churn-Jung Liau, Da-Wei Wang, Jeremy K.-P. Chen

A New Offline Privacy Protecting E-cash System with Revokable Anonymity 177
Weidong Qiu, Kefei Chen, Dawu Gu

E-commerce Protocols (I)

Receipt-Free Sealed-Bid Auction 191
Masayuki Abe, Koutarou Suzuki

Exclusion-Freeness in Multi-party Exchange Protocols 200
Nicolás González-Deleito, Olivier Markowitch

A Realistic Protocol for Multi-party Certified Electronic Mail 210
Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, Llorenç Huguet-Rotger

Signature Schemes

A Nyberg-Rueppel Signature for Multiple Messages and Its Batch Verification 220
Shunsuke Araki

Comments to the UNCITRAL Model Law on Electronic Signatures 229
Apol·lònia Martínez-Nadal, Josep Lluís Ferrer-Gomila

An Anonymous Loan System Based on Group Signature Scheme 244
Rie Shigetomi, Akira Otsuka, Takahide Ogawa, Hideki Imai

Traceability Schemes for Signed Documents 257
Shoko Yonezawa, Goichiro Hanaoka, Junji Shikata, Hideki Imai

Cryptography (I)

Proofs of Knowledge for Non-monotone Discrete-Log Formulae and Applications 272
Emmanuel Bresson, Jacques Stern

Inversion/Division Systolic Architecture for Public-Key Cryptosystems in GF(2^m) 289
Nam-Yeun Kim, Dae-Ghon Kho, Kee-Young Yoo

Efficient Bit Serial Multiplication Using Optimal Normal Bases of Type II in $GF(2^m)$ 300
Soonhak Kwon, Heuisu Ryu

Access Control and Trust Management (II)

Conditional Cryptographic Delegation for P2P Data Sharing 309
Yuji Watanabe, Masayuki Numao

Certification of Public Keys within an Identity Based System 322
L. Chen, K. Harrison, A. Moss, D. Soldera, N.P. Smart

A New Public Key Cryptosystem for Constrained Hardware 334
Jiande Zheng

Key Management

A Distributed and Computationally Secure Key Distribution Scheme 342
Vanesa Daza, Javier Herranz, Carles Padró, Germán Sáez

On Optimal Hash Tree Traversal for Interval Time-Stamping 357
Helger Lipmaa

An Efficient Dynamic and Distributed Cryptographic Accumulator 372
Michael T. Goodrich, Roberto Tamassia, Jasminka Hasić

Security Analysis

A Second-Order DPA Attack Breaks a Window-Method Based Countermeasure against Side Channel Attacks 389
Katsuyuki Okeya, Kouichi Sakurai

Parallelizable Elliptic Curve Point Multiplication Method with Resistance against Side-Channel Attacks 402
Bodo Möller

Automated Analysis of Some Security Mechanisms of SCEP 414
Fabio Martinelli, Marinella Petrocchi, Anna Vaccarelli

An Attack on a Protocol for Certified Delivery 428
José R.M. Monteiro, Ricardo Dahab

E-commerce Protocols (II)

Oblivious Counter and Majority Protocol 437
Hiroaki Kikuchi

Efficient Mental Card Shuffling via Optimised Arbitrary-Sized Benes Permutation Network 446
Wai Han Soo, Azman Samsudin, Alwyn Goh

Fingerprinting Concatenated Codes with Efficient Identification 459
M. Fernandez, M. Soriano

Cryptography (II)

A Provably Secure Additive and Multiplicative Privacy Homomorphism 471
Josep Domingo-Ferrer

Algorithms for Efficient Simultaneous Elliptic Scalar Multiplication with Reduced Joint Hamming Weight Representation of Scalars 484
Yasuyuki Sakai, Kouichi Sakurai

Author Index 501