

Lecture Notes in Computer Science

2200

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

George I. Davida Yair Frankel (Eds.)

Information Security

4th International Conference, ISC 2001
Malaga, Spain, October 1-3, 2001
Proceedings



Springer

Series Editors

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

Volume Editors

George I. Davida
University of Wisconsin-Milwaukee, Department of EECS
Milwaukee, WI 53201, USA
E-mail: davida@cs.uwm.edu

Yair Frankel
Techtegrity, LLC
122 Harrison, Westfield NJ 07090, USA
E-mail: yfrankel@cryptographers.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : 4th international conference ; proceedings / ISC
2001, Malaga, Spain, October 1 - 3, 2001. George I. Davida ; Yair Frankel
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2200)
ISBN 3-540-42662-0

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.2.1, C.2, J.1, C.3

ISSN 0302-9743

ISBN 3-540-42662-0 Springer-Verlag Berlin Heidelberg New York

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. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10840698 06/3142 5 4 3 2 1 0

Preface

The Information Security Conference 2001 brought together individuals involved in multiple disciplines of information security to foster the exchange of ideas. The conference, an outgrowth of the Information Security Workshop (ISW) series, was held in Málaga, Spain, on October 1–3, 2001. Previous workshops were ISW '97 at Ishikawa, Japan; ISW '99 at Kuala Lumpur, Malaysia; and ISW 2000 at Wollongong, Australia. The General Co-chairs, Javier López and Eiji Okamoto, oversaw the local organization, registration, and performed many other tasks.

Many individuals deserve thanks for their contribution to the success of the conference. José M. Troya was the Conference Chair. The General Co-chairs were assisted with local arrangements by Antonio Maña, Carlos Maraval, Juan J. Ortega, José M. Sierra, and Miguel Soriano.

This was the first year that the conference accepted electronic submissions. Many thanks to Dawn Gibson for assisting in developing and maintaining the electronic submission servers. The conference received 98 submissions of which 37 papers were accepted for presentation. These proceedings contain revised versions of the accepted papers. Revisions were not checked and the authors bear full responsibility for the contents of their papers.

The Program Committee consisted of Elisa Bertino, Università di Milano; G. R. Blakely, Texas A&M University; John Daugman, Cambridge University; Jorge Dávila, Polytechnic Univ. of Madrid; Giovanni DiCrescenzo, Telcordia; Josep Domingo-Ferrer, Univ. Rovira i Virgili; Dieter Gollmann, Microsoft Research; Sigrid Guergens, GMD; Hiroaki Kikuchi, Tokai University; Chi-Sung Lai, Natl. Cheng Kung Univ.; Wenbo Mao, HP Laboratories; Masahiro Mambo, Tohoku University; Catherine Meadows, NRL; Sang-Jae Moon, Kyungpook Natl. University; Yuko Murayama, Iwate Prefectural University; René Peralta, Yale University; Josef Pieprzyk, University of Wollongong; Sihan Qing, Chinese Academy of Sciences; Susie Thomson, Datacard; Routo Terada, Univ. of S. Paulo; Yiannis Tsiounis, InternetCash; Moti Yung, Certco; Yuliang Zheng, Monash University; Jianying Zhou, Oracle Corp. Members of the committee spent numerous hours in reviewing papers and providing advice. The committee was also assisted by our colleagues: Marc Alba, Clemente Galdi, Sang-Wook Kim, Yi Mu, Anna Oganian, Francesc Sebé, Rajan Shankaran, Igor Shparlinski. We apologize for any inadvertent omissions. Our thanks to the program committee and all reviewers.

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

July 2001

George I. Davida
Yair Frankel

Information Security Conference 2001

October 1–3, 2001, Málaga, Spain

Conference Chair

José M. Troya, University of Málaga (Spain)

General Co-chairs

Javier López, University of Málaga (Spain)

Eiji Okamoto, Toho University (Japan)

Program Co-chair

George I. Davida, University of Wisconsin-Milwaukee (USA)

Yair Frankel, TechTegrity L.L.C. (USA)

Program Committee

Elisa Bertino Università di Milano (Italy)
G. R. Blakely..... Texas A&M University (USA)
John DaugmanCambridge University (UK)
Jorge DávilaPolytechnic Univ. of Madrid (Spain)
Giovanni DiCrescenzo Telcordia (USA)
Josep Domingo-Ferrer..... Univ. Rovira i Virgili (Spain)
Dieter Gollmann.....Microsoft Research (UK)
Sigrid GuergensGMD (Germany)
Hiroaki KikuchiTokai University (Japan)
Chi-Sung Laih.....Natl. Cheng Kung Univ. (Taiwan)
Wenbo Mao.....HP Laboratories (UK)
Masahiro Mambo Tohoku University (Japan)
Catherine Meadows.....NRL (USA)
Sang-Jae MoonKyungpook Natl. University (Korea)
Yuko MurayamaIwate Prefectural University (Japan)
Rene Peralta Yale University (USA)
Josef Pieprzyk University of Wollongong (Australia)
Si-han Qing Chinese Academy of Sciences (China)
Susie Thomson..... Datacard (UK)
Routo Terada..... Univ. of S. Paulo (Brazil)
Yiannis Tsiounis InternetCash (USA)
Moti Yung..... CertCo (USA)
Yuliang ZhengMonash University (Australia)
Jianying Zhou Oracle Corp. (USA)

Table of Contents

Key Distribution

Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures	1
<i>Carlo Blundo, Paolo D'Arco (Università di Salerno)</i> <i>Vanessa Daza, and Carles Padró (Universitat Politècnica de Catalunya)</i>	
Privacy Amplification Theorem for Noisy Main Channel	18
<i>Valeri Korjik, Guillermo Morales-Luna (CINVESTAV-IPN),</i> <i>and Vladimir B. Balakirsky (EIDMA)</i>	

Protocols

Efficient Kerberized Multicast in a Practical Distributed Setting.....	27
<i>Giovanni Di Crescenzo (Telcordia Technologies)</i> <i>and Olga Kornievskaia (University of Michigan)</i>	
Suitability of a Classical Analysis Method for E-commerce Protocols.....	46
<i>Sigrid Gürgens (GMD-SIT) and Javier Lopez (University of Malaga)</i>	

Enhancing Technologies

Hypocrites (A New Proactive Password Checker)	63
<i>Carlo Blundo, Paolo D'Arco, Alfredo De Santis,</i> <i>and Clemente Galdi (Università di Salerno)</i>	
Lenient/Strict Batch Verification in Several Groups	81
<i>Fumitaka Hoshino, Masayuki Abe,</i> <i>and Tetsutaro Kobayashi (NTT Corporation)</i>	

Privacy

Absolute Privacy in Voting	95
<i>Dmitri Asonov (Humboldt-Universität zu Berlin),</i> <i>Markus Schaal (Technische Universität Berlin), and</i> <i>Johann-Christoph Freytag (Humboldt-Universität zu Berlin)</i>	
A Logical Model for Privacy Protection	110
<i>Tsan-sheng Hsu, Churn-Jung Liao,</i> <i>and Da-Wei Wang (Academia Sinica)</i>	

Software Protection

DISSECT: DIStribution for SECurity Tool	125
<i>Enriquillo Valdez (Polytechnic University of New York)</i> <i>and Moti Yung (CertCo, Inc.)</i>	
An Approach to the Obfuscation of Control-Flow of Sequential Computer Programs	144
<i>Stanley Chow, Yuan Gu, Harold Johnson (Cloakware Corporation),</i> <i>and Vladimir A. Zakharov (Moscow State University)</i>	

Message Hiding I

A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography	156
<i>Mark Chapman (Omni Tech Corp.),</i> <i>George I. Davida (University of Wisconsin-Milwaukee), and</i> <i>Marc Rennhard (Swiss Federal Institute of Technology)</i>	
Robust New Method in Frequency Domain Watermarking	166
<i>David Sánchez, Agustín Orfila, Julio César Hernández,</i> <i>and José María Sierra (Carlos III University)</i>	

PKI Issues and Protocols

On the Complexity of Public-Key Certificate Validation	183
<i>Diana Berbecaru, Antonio Lioy, and</i> <i>Marius Marian (Politecnico di Torino)</i>	
Liability of Certification Authorities: A Juridical Point of View	204
<i>Apol·lònia Martínez-Nadal and</i> <i>Josep L. Ferrer-Gomila (Universitat de les Illes Balears)</i>	

Hardware Implementations

Experimental Testing of the Gigabit IPSec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board	220
<i>Pawel Chodowiec, Kris Gaj (George Mason University),</i> <i>Peter Bellows, and Brian Schott (University of Southern California)</i>	
Elliptic Curve Arithmetic Using SIMD	235
<i>Kazumaro Aoki (NTT Communications), Fumitaka Hoshino,</i> <i>Tetsutaro Kobayashi, and Hiroaki Oguro (NTT Corporation)</i>	

On the Hardware Implementation of the 3GPP Confidentiality and Integrity Algorithms	248
<i>Kostas Marinis (National Technical University of Athens), Nikos K. Moshopoulos, Fotis Karoubalis (Atmel Hellas), and Kiamal Z. Pekmestzi (National Technical University of Athens)</i>	
Efficient Implementation of Elliptic Curve Cryptosystems on an ARM7 with Hardware Accelerator	266
<i>Sheng-Bo Xu and Lejla Batina (Securealink B.V.)</i>	

Cryptanalysis and Prevention

A Theoretical DPA-Based Cryptanalysis of the NESSIE Candidates FLASH and SFLASH.....	280
<i>Rainer Steinwandt, Willi Geiselmann, and Thomas Beth (Universität Karlsruhe)</i>	
Quadratic Relations for S-Boxes: Their Minimum Representations and Bounds	294
<i>Routo Terada and Paulo G. Pinheiro (University of S. Paulo)</i>	
Approximate Power Roots in $\mathbb{Z}_m$	310
<i>Ismael Jiménez-Calvo (C.S.I.C.) and German Sáez-Moreno (Universitat Politècnica de Catalunya)</i>	
Securing Elliptic Curve Point Multiplication against Side-Channel Attacks	324
<i>Bodo Möller (Technische Universität Darmstadt)</i>	

Implementations

A Flexible Role-Based Access Control Model for Multimedia Medical Image Database Systems	335
<i>Sofia Tzelepi and George Pangalos (Aristotelian University)</i>	
A Secure Publishing Service for Digital Libraries of XML Documents	347
<i>Elisa Bertino, Barbara Carminati (Università di Milano), and Elena Ferrari (Università dell'Insubria)</i>	

Non-repudiation Techniques

An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party	363
<i>Olivier Markowitch and Steve Kremer (Université Libre de Bruxelles)</i>	

Persistent Authenticated Dictionaries and Their Applications	379
<i>Aris Anagnostopoulos (Brown University), Michael T. Goodrich (University of California), and Roberto Tamassia (Brown University)</i>	

Contracts and Auctions

Efficient Optimistic N-Party Contract Signing Protocol	394
<i>Josep L. Ferrer-Gomila, Magdalena Payeras-Capellà, and Llorenç Huguet-Rotger (Universitat de les Illes Balears)</i>	
Efficient Sealed-Bid Auctions for Massive Numbers of Bidders with Lump Comparison	408
<i>Koji Chida, Kunio Kobayashi, and Hikaru Morita (NTT Corporation)</i>	

Message Hiding II

Oblivious Image Watermarking Robust against Scaling and Geometric Distortions	420
<i>Francesc Sebé and Josep Domingo-Ferrer (Universitat Rovira i Virgili)</i>	
Fingerprinting Text in Logical Markup Languages	433
<i>Christian D. Jensen (Trinity College Dublin)</i>	

Payments

SPEED Protocol: Smartcard-Based Payment with Encrypted Electronic Delivery	446
<i>Antonio Ruiz, Gregorio Martínez, Oscar Cánovas, and Antonio F. Gómez (University of Murcia)</i>	
Efficient Transferable Cash with Group Signatures	462
<i>Ik Rae Jeong, Dong Hoon Lee, and Jong In Lim (Korea University)</i>	

Security Applications

An Auditable Metering Scheme for Web Advertisement Applications	475
<i>Liqun Chen and Wenbo Mao (Hewlett-Packard Laboratories)</i>	

Broker-Based Secure Negotiation of Intellectual Property Rights	486
<i>Jaime Delgado (Universitat Pompeu Fabra), Isabel Gallego</i>	
<i>(Universitat Politècnica de Catalunya), and Xavier Perramon</i>	
<i>(Universitat Pompeu Fabra)</i>	

Network and OS Security

Design of the Decision Support System for Network Security	
Management to Secure Enterprise Network	497
<i>Jae Seung Lee (ETRI) and</i>	
<i>Sang Choon Kim (Samchok National University)</i>	

Measuring False-Positive by Automated Real-Time Correlated Hacking	
Behavior Analysis	512
<i>Jia Wang and Insup Lee (University of Pennsylvania)</i>	

Design of UNIX System for the Prevention of Damage Propagation	
by Intrusion and Its Implementation Based on 4.4BSD	536
<i>Kenji Masui, Masahiko Tomoishi,</i>	
<i>and Naoki Yonezaki (Tokyo Institute of Technology)</i>	

Author Index	553
---------------------------	------------