

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Kan Zhang Yuliang Zheng (Eds.)

Information Security

7th International Conference, ISC 2004
Palo Alto, CA, USA, September 27-29, 2004
Proceedings



Springer

Volume Editors

Kan Zhang
Hewlett-Packard Laboratories
3353 Alma Street, #233, Palo Alto, CA 94306, USA
E-mail: zhangkan@sbcglobal.net

Yuliang Zheng
University of North Carolina at Charlotte
Department of Software and Information Systems
9201 University City Blvd, Charlotte, NC 28223, USA
E-mail: yzheng@uncc.edu

Library of Congress Control Number: 2004112165

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

ISSN 0302-9743

ISBN 3-540-23208-7 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11325864 06/3142 5 4 3 2 1 0

Preface

The 2004 Information Security Conference was the seventh in a series that started with the Information Security Workshop in 1997. A distinct feature of this series is the wide coverage of topics with the aim of encouraging interaction between researchers in different aspects of information security. This trend continued in the program of this year's conference. The program committee received 106 submissions, from which 36 were selected for presentation. Each submission was reviewed by at least three experts in the relevant research area. We would like to thank all the authors for taking their time to prepare the submissions, and we hope that those whose papers were declined will be able to find an alternative forum for their work.

We were fortunate to have an energetic team of experts who took on the task of the program committee. Their names may be found overleaf, and we thank them warmly for their time and efforts. This team was helped by an even larger number of external reviewers who reviewed papers in their particular areas of expertise. A list of these names is also provided, which we hope is complete.

We would also like to thank the advisory committee for their advice and support. The excellent local arrangements were handled by Dirk Balfanz and Jessica Staddon. We made use of the electronic submission and reviewing software supplied by COSIC at the Katholieke Universiteit Leuven. Both the software and the ISC 2004 website were run on a server at UNC Charlotte, and were perfectly maintained by Seung-Hyun Im. We also appreciate assistance from Lawrence Teo in editing the proceedings.

September 2004

Kan Zhang
Yuliang Zheng

Information Security Conference 2004

September 27–29, 2004, Palo Alto, CA, USA

General Chair

Yuliang Zheng, University of North Carolina at Charlotte, USA

Advisory Committee

Tom Berson, Anagram Lab, USA

Li Gong, Sun Microsystems, China

Wenbo Mao, Hewlett-Packard Laboratories, UK

Eiji Okamoto, University of Tsukuba, Japan

Program Co-chairs

Kan Zhang, Hewlett-Packard Laboratories, USA

Yuliang Zheng, University of North Carolina at Charlotte, USA

Program Committee

Martin Abadi	UC Santa Cruz, USA
Carlisle Adams	University of Ottawa, Canada
Gail-Joon Ahn	UNC Charlotte, USA
N. Asokan	Nokia, Finland
Tuomas Aura	Microsoft Research, UK
Jean Bacon	Cambridge University, UK
Dirk Balfanz	PARC, USA
Feng Bao	i2r, Singapore
Elisa Bertino	University of Milan, Italy
Colin Boyd	QUT, Australia
Yvo Desmedt	University College London, UK
Warwick Ford	Verisign, USA
Craig Gentry	NTT DoCoMo Labs, USA
Stuart Haber	HP Labs, USA
Markus Jakobsson	RSA Labs, USA
Marc Joye	Gemplus, France
Michiharu Kudoh	IBM Tokyo, Japan
Javier Lopez	University of Malaga, Spain
Tsutomu Matsumoto	Yokohama National University, Japan
Kanta Matsuura	University of Tokyo, Japan
Catherine Meadows	Naval Research Lab, USA
Jonathan Millen	SRI International, USA
John Mitchell	Stanford University, USA
Peng Ning	North Carolina State University, USA
Joe Pato	HP Labs, USA
Josef Pieprzyk	Macquarie University, Australia
Jean-Jacques Quisquater	UCL, Belgium

Michael Reiter	CMU, USA
Scarlet Schwiderski-Grosche	Royal Holloway, University of London, UK
Hovav Shacham	Stanford University, USA
Dawn Song	CMU, USA
Jessica Staddon	PARC, USA
Clark Thomborson	University of Auckland, New Zealand
Serge Vaudenay	EPFL, Switzerland
Michael Waidner	IBM Research, Switzerland
Yumin Wang	Xidian University, China
Moti Yung	Columbia University, USA
Kan Zhang	HP Labs, USA
Yuliang Zheng	UNC Charlotte, USA
Jianying Zhou	i2r, Singapore

External Reviewers

Giuseppe Ateniese	Zhenjie Huang	Diana Smetters
Joonsang Baek	Zhengtao Jiang	Mike Stay
Thomas Baigneres	Pascal Junod	Ron Steinfeld
Julien Bouchier	Jonathan Katz	Paul Syverson
Julien Cathalo	Yongdae Kim	Anat Talmy
Mathieu Ciet	Mei Kobayashi	Lawrence Teo
Scott Contini	Tieyan Li	Haibo Tian
Nora Dabbous	Yi Lu	Gene Tsudik
Chen Dan	Benjamin Lynn	Chenxi Wang
Tanmoy Das	Greg Maitland	Guilin Wang
Alex Deacon	Krystian Matusiewicz	Huaxiong Wang
Anand Desai	Keith Mayes	Bogdan Warinschi
Glenn Durfee	Bruce Mills	Claire Whelan
Dan DuVarney	Jean Monnerat	Nathan Whitehead
Tim Ebringer	Jose A. Montenegro	Hao Chi Wong
Hiroaki Etoh	Sara Miner More	Yongdong Wu
Serge Fehr	Ram Moskovitz	Dingbang Xu
Dan Forsberg	Zhihua Niu	Mariemma I. Yague
Michael J. Freedman	Juan J. Ortega	Adam Young
Steven Galbraith	Olivier Pereira	Ting Yu
Vaibhav Gowadia	Gilles Piret	John Zachary
Phillip Hallam-Baker	Zulfikar Ramzan	Jianhong Zhang
Thomas Hardjono	Louis Salvail	

Table of Contents

Key Management

Practical Authenticated Key Agreement Using Passwords	1
<i>Taekyoung Kwon</i>	
Further Analysis of Password Authenticated Key Exchange Protocol Based on RSA for Imbalanced Wireless Networks	13
<i>Muxiang Zhang</i>	
Storage-Efficient Stateless Group Key Revocation	25
<i>Pan Wang, Peng Ning, Douglas S. Reeves</i>	

Digital Signatures

Low-Level Ideal Signatures and General Integrity Idealization	39
<i>Michael Backes, Birgit Pfitzmann, Michael Waidner</i>	
Cryptanalysis of a Verifiably Committed Signature Scheme Based on GPS and RSA	52
<i>Julien Cathalo, Benoît Libert, Jean-Jacques Quisquater</i>	
How to Break and Repair a Universally Composable Signature Functionality	61
<i>Michael Backes, Dennis Hofheinz</i>	

New Algorithms

RSA Accumulator Based Broadcast Encryption	73
<i>Craig Gentry, Zulfikar Ramzan</i>	
Chameleon Hashing Without Key Exposure	87
<i>Xiaofeng Chen, Fangguo Zhang, Kwangjo Kim</i>	
Radix- r Non-Adjacent Form	99
<i>Tsuyoshi Takagi, Sung-Ming Yen, Bo-Ching Wu</i>	

Cryptanalysis

On Related-Key and Collision Attacks: The Case for the IBM 4758 Cryptoprocessor	111
<i>Raphael C.-W. Phan, Helena Handschuh</i>	
Security Analysis of Two Signcryption Schemes	123
<i>Guilin Wang, Robert H. Deng, DongJin Kwak, SangJae Moon</i>	

On The Security of Key Derivation Functions	134
<i>Carlisle Adams, Guenther Kramer, Serge Mister, Robert Zuccherato</i>	

Intrusion Detection

Evaluating the Impact of Intrusion Detection Deficiencies on the Cost-Effectiveness of Attack Recovery	146
<i>Hai Wang, Peng Liu, Lunqun Li</i>	
A Model for the Semantics of Attack Signatures in Misuse Detection Systems	158
<i>Michael Meier</i>	
Detection of Sniffers in an Ethernet Network	170
<i>Zouheir Trabelsi, Hamza Rahmani</i>	
Using Greedy Hamiltonian Call Paths to Detect Stack Smashing Attacks	183
<i>Mark Foster, Joseph N. Wilson, Shigang Chen</i>	
Securing DBMS: Characterizing and Detecting Query Floods	195
<i>Elisa Bertino, Teodoro Leggieri, Evimaria Terzi</i>	

Access Control

An XML-Based Approach to Document Flow Verification	207
<i>Elisa Bertino, Elena Ferrari, Giovanni Mella</i>	
Model-Checking Access Control Policies	219
<i>Dimitar P. Guelev, Mark Ryan, Pierre Yves Schobbens</i>	
A Distributed High Assurance Reference Monitor	231
<i>Ajay Chander, Drew Dean, John Mitchell</i>	
Using Mediated Identity-Based Cryptography to Support Role-Based Access Control	245
<i>D. Nali, C. Adams, A. Miri</i>	

Human Authentication

Towards Human Interactive Proofs in the Text-Domain (Using the Problem of Sense-Ambiguity for Security)	257
<i>Richard Bergmair, Stefan Katzenbeisser</i>	
Image Recognition CAPTCHAs	268
<i>Monica Chew, J.D. Tygar</i>	

Certificate Management

A Hierarchical Key-Insulated Signature Scheme in the CA Trust Model	280
<i>Zhengyi Le, Ouyang Yi, James Ford, Fillia Makedon</i>	
Certificate Recommendations to Improve the Robustness of Web of Trust	292
<i>Qinglin Jiang, Douglas S. Reeves, Peng Ning</i>	

Mobile and Ad Hoc Security

Universally Composable Secure Mobile Agent Computation	304
<i>Ke Xu, Stephen R. Tate</i>	
Re-thinking Security in IP Based Micro-Mobility	318
<i>Jukka Ylitalo, Jan Melén, Pekka Nikander, Vesa Torvinen</i>	
Shared-Key Signature and Its Application to Anonymous Authentication in Ad Hoc Group	330
<i>Qianhong Wu, Xiaofeng Chen, Changjie Wang, Yumin Wang</i>	

Web Security

Prevent Online Identity Theft – Using Network Smart Cards for Secure Online Transactions	342
<i>HongQian Karen Lu, Asad Ali</i>	
Provable Unlinkability Against Traffic Analysis Already After $\mathcal{O}(\log(n))$ Steps!	354
<i>Marcin Gomułkiewicz, Marek Klonowski, Mirosław Kutylowski</i>	
An Efficient Online Electronic Cash with Unlinkable Exact Payments	367
<i>Toru Nakanishi, Mitsuaki Shiota, Yuji Sugiyama</i>	

Digital Rights Management

Modifiable Digital Content Protection in P2P	379
<i>Heejae Park, Jong Kim</i>	
Survey on the Technological Aspects of Digital Rights Management	391
<i>William Ku, Chi-Hung Chi</i>	
Detecting Software Theft via Whole Program Path Birthmarks	404
<i>Ginger Myles, Christian Collberg</i>	

Software Security

Effective Security Requirements Analysis: HAZOP and Use Cases	416
<i>Thitima Srivatanakul, John A. Clark, Fiona Polack</i>	

The Obfuscation Executive 428
 Kelly Heffner, Christian Collberg

Author Index 441