

Lecture Notes in Computer Science

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

2119

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Vijay Varadharajan Yi Mu (Eds.)

Information Security and Privacy

6th Australasian Conference, ACISP 2001
Sydney, Australia, July 11-13, 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

Vijay Varadharajan
Yi Mu
Macquarie University, Department of Computing
North Ryde, NSW 2109, Australia
E-mail: {vijay,ymu}@ics.mq.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : 6th Australasian conference ; proceedings
/ ACISP 2001, Sydney, Australia, July 11 - 13, 2001. Vijay Varadharajan ; Yi
Mu (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2119)
ISBN 3-540-42300-1

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743

ISBN 3-540-42300-1 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 Boller Mediendesign
Printed on acid-free paper SPIN: 10839883 06/3142 5 4 3 2 1 0

Preface

ACISP 2001, the Sixth Australasian Conference on Information Security and Privacy, was held in Sydney, Australia. The conference was sponsored by Information and Networked System Security Research (INSSR), Macquarie University, the Australian Computer Society, and the University of Western Sydney. I am grateful to all these organizations for their support of the conference.

The aim of this conference was to draw together researchers, designers, and users of information security systems and technologies. The conference program addressed a range of aspects from system and network security to secure Internet applications to cryptography and cryptanalysis. This year the program committee invited two international keynote speakers Dr. Yacov Yacobi from Microsoft Research (USA) and Dr. Clifford Neumann from the University of Southern California (USA). Dr. Yacobi's talk addressed the issues of trust, privacy, and anti-piracy in electronic commerce. Dr. Neumann's address was concerned with authorization policy issues and their enforcement in applications.

The conference received 91 papers from America, Asia, Australia, and Europe. The program committee accepted 38 papers and these were presented in some 9 sessions covering system security, network security, trust and access control, Authentication, cryptography, cryptanalysis, Digital Signatures, Elliptic Curve Based Techniques, and Secret Sharing and Threshold Schemes. This year the accepted papers came from a range of countries, including 7 from Australia, 8 from Korea, 7 from Japan, 3 from UK, 3 from Germany, 3 from USA, 2 from Singapore, 2 from Canada and 1 from Belgium, Estonia, and Taiwan.

Organizing a conference such as this one is a time-consuming task and I would like to thank all the people who worked hard to make this conference a success. In particular, I would like to thank Program Co-chair Yi Mu for his tireless work and the members of the program committee for putting together an excellent program, and all the session chairs and speakers for their time and effort. Special thanks to Yi Mu, Laura Olsen, Rajan Shankaran, and Michael Hitchens for their help with local organization details. Finally, I would like to thank all the authors who submitted papers and all the participants of ACISP 2001. I hope that the professional contacts made at this conference, the presentations, and the proceedings have offered you insights and ideas that you can apply to your own efforts in security and privacy.

AUSTRALASIAN CONFERENCE ON INFORMATION SECURITY AND PRIVACY ACISP 2001

Sponsored by
Macquarie University
Australian Computer Society

General Chair:

Vijay Varadharajan

Macquarie University, Australia

Program Chairs:

Vijay Varadharajan
Yi Mu

Macquarie University, Australia
Macquarie University, Australia

Program Committee:

Ross Anderson
Colin Boyd
Ed Dawson
Yvo Desmedt
Paul England
Yair Frankel
Ajoy Ghosh
Dieter Gollman
John Gordon
Kwangjo Kim
Chuchang Liu
Masahiro Mambo
Wenbo Mao
Chris Mitchell
Eiji Okamoto
Joe Pato
Josef Pieprzyk
Bart Preneel
Steve Roberts
Qing Sihan
Rei Safavi-Naini
Jennifer Seberry
Yuliang Zheng

Cambridge University, UK
Queensland University of Technology, Australia
Queensland University of Technology, Australia
Florida State University, USA
Microsoft
Columbia University, USA
UNISYS, Australia
Microsoft
ConceptLabs, UK
ICU, Korea
DSTO, Australia
Tohoku University, Japan
Hewlett-Packard Lab., UK
London University, UK
University of Wisconsin, USA
Hewlett-Packard Lab., USA
Macquarie University, Australia
Katholieke University, Belgium
Witham Pty Ltd, Australia
Academy of Science, China
University of Wollongong, Australia
University of Wollongong, Australia
Monash University, Australia

Table of Contents

A Few Thoughts on E-Commerce	1
<i>Yacov Yacobi</i>	
New CBC-MAC Forgery Attacks	3
<i>Karl Brincat, Chris J. Mitchell</i>	
Cryptanalysis of a Public Key Cryptosystem Proposed at ACISP 2000	15
<i>Amr Youssef, Guang Gong</i>	
Improved Cryptanalysis of the Self-Shrinking Generator	21
<i>Erik Zenner, Matthias Krause, Stefan Lucks</i>	
Attacks Based on Small Factors in Various Group Structures	36
<i>Chris Pavlovski, Colin Boyd</i>	
On Classifying Conference Key Distribution Protocols	51
<i>Shahrokh Saeednia, Rei Safavi-Naini, Willy Susilo</i>	
Pseudorandomness of MISTY-Type Transformations and the Block Cipher KASUMI	60
<i>Ju-Sung Kang, Okyeon Yi, Dowon Hong, Hyunsook Cho</i>	
New Public-Key Cryptosystem Using Divisor Class Groups	74
<i>Hwankoo Kim, SangJae Moon</i>	
First Implementation of Cryptographic Protocols Based on Algebraic Number Fields	84
<i>Andreas Meyer, Stefan Neis, Thomas Pfahler</i>	
Practical Key Recovery Schemes	104
<i>Sung-Ming Yen</i>	
Non-deterministic Processors	115
<i>David May, Henk L. Muller, Nigel P. Smart</i>	
Personal Secure Booting	130
<i>Naomaru Itoi, William A. Arbaugh, Samuela J. Pollack, Daniel M. Reeves</i>	
Evaluation of Tamper-Resistant Software Deviating from Structured Programming Rules	145
<i>Hideaki Goto, Masahiro Mambo, Hiroki Shizuya, Yasuyoshi Watanabe</i>	
A Strategy for MLS Workflow	159
<i>Vlad Ingar Wietrzyk, Makoto Takizawa, Vijay Varadharajan</i>	

Condition-Driven Integration of Security Services	176
<i>Clifford Neumann</i>	
SKETHIC: Secure Kernel Extension against Trojan Horses with Information-Carrying Codes	177
<i>Eun-Sun Cho, Sunho Hong, Sechang Oh, Hong-Jin Yeh, Manpyo Hong, Cheol-Won Lee, Hyundong Park, Chun-Sik Park</i>	
Secure and Private Distribution of Online Video and Some Related Cryptographic Issues	190
<i>Feng Bao, Robert Deng, Peirong Feng, Yan Guo, Hongjun Wu</i>	
Private Information Retrieval Based on the Subgroup Membership Problem	206
<i>Akihiro Yamamura, Taiichi Saito</i>	
A Practical English Auction with One-Time Registration	221
<i>Kazumasa Omote, Atsuko Miyaji</i>	
A User Authentication Scheme with Identity and Location Privacy	235
<i>Shouichi Hirose, Susumu Yoshida</i>	
An End-to-End Authentication Protocol in Wireless Application Protocol .	247
<i>Jong-Phil Yang, Weon Shin, Kyung-Hyune Rhee</i>	
Error Detection and Authentication in Quantum Key Distribution	260
<i>Akihiro Yamamura, Hirokazu Ishizuka</i>	
An Axiomatic Basis for Reasoning about Trust in PKIs	274
<i>Chuchang Liu, Maris Ozols, Tony Cant</i>	
A Knowledge-Based Approach to Internet Authorizations	292
<i>Along Lin</i>	
Applications of Trusted Review to Information Security	305
<i>John Yesberg, Marie Henderson</i>	
Network Security Modeling and Cyber Attack Simulation Methodology ...	320
<i>Sung-Do Chi, Jong Sou Park, Ki-Chan Jung, Jang-Se Lee</i>	
Cryptographic Salt: A Countermeasure against Denial-of-Service Attacks..	334
<i>DongGook Park, JungJoon Kim, Colin Boyd, Ed Dawson</i>	
Enhanced Modes of Operation for the Encryption in High-Speed Networks and Their Impact on QoS	344
<i>Oliver Jung, Sven Kuhn, Christoph Ruland, Kai Wollenweber</i>	
Improving the Availability of Time-Stamping Services	360
<i>Arne Ansper, Ahto Buldas, Märt Saarepera, Jan Willemsen</i>	

Randomness Required for Linear Threshold Sharing Schemes Defined over Any Finite Abelian Group	376
<i>Brian King</i>	
Democratic Systems	392
<i>Hossein Ghodosi, Josef Pieprzyk</i>	
Efficient and Unconditionally Secure Verifiable Threshold Changeable Scheme	403
<i>Ayako Maeda, Atsuko Miyaji, Mitsuru Tada</i>	
Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold Scheme for Implicit Certificates	417
<i>Douglas R. Stinson, Reto Stroh</i>	
How to Construct Fail-Stop Confirmer Signature Schemes	435
<i>Rei Safavi-Naini, Willy Susilo, Huaxiong Wang</i>	
Signature Schemes Based on 3rd Order Shift Registers	445
<i>Chik How Tan, Xun Yi, Chee Kheong Siew</i>	
Anonymous Statistical Survey of Attributes	460
<i>Toru Nakanishi, Yuji Sugiyama</i>	
Secure Mobile Agent Using Strong Non-designated Proxy Signature	474
<i>Byoungcheon Lee, Heesun Kim, Kwangjo Kim</i>	
Elliptic Curve Based Password Authenticated Key Exchange Protocols ...	487
<i>Colin Boyd, Paul Montague, Khanh Nguyen</i>	
Elliptic Curve Cryptography on a Palm OS Device	502
<i>André Weimerskirch, Christof Paar, Sheueling Chang Shantz</i>	
Reducing Certain Elliptic Curve Discrete Logarithms to Logarithms in a Finite Field	514
<i>Kyungah Shim</i>	
Author Index	521