Lecture Notes in Computer Science 1438
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Colin Boyd Ed Dawson (Eds.)

Information Security and Privacy

Third Australasian Conference, ACISP'98
Brisbane, Australia, July 13-15, 1998
Proceedings

Springer

Volume Editors

Colin Boyd
Ed Dawson
Information Security Research Centre
Queensland University of Technology
2 George Street, Brisbane Q 4001, Australia
E-mail: {boyd,dawson}@fit.qut.edu.au

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : third Australasian conference ; proceedings / ACISP '98, Brisbane, Australia, July 13 - 15, 1998. Ed Dawson ; Colin Boyd (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1438)
ISBN 3-540-64732-5

CR Subject Classification (1991): E.3, K.6.5, D.4.6, C.2, E.4,F.2.1-2, K.4.1

ISSN 0302-9743
ISBN 3-540-64732-5 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10637980 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

ACISP'98, the Third Australasian Conference on Information Security and Privacy, was held in Brisbane, Australia, July 13–15 1998. The conference was sponsored by the Information Security Research Centre at Queensland University of Technology, the Australian Computer Society, ERACOM Pty Ltd, and Media Tech Pacific Pty Ltd. We are grateful to all these organizations for their support of the conference.

The conference brought together researchers, designers, implementors and users of information security systems. The aim of the conference is to have a series of technical refereed and invited papers to discuss all different aspects of information security. The Program Committee invited four distinguished speakers: Doug McGowan, Per Kaijser, Winfried Müller, and William Caelli. Doug McGowan from Hewlett Packard Company presented a paper entitled "Cryptography in an international environment: It just might be possible!"; Per Kaijser from Siemens presented a paper entitled "A review of the SESAME development"; Winfried Müller from University of Klagenfurt in Austria presented a paper entitled "The security of public key cryptosystems based on integer factorization"; and William Caelli from Queensland University of Technology presented a paper entitled "CIP versus CRYP: Critical infrastructure protection and the cryptography policy debate".

There were sixty-six technical papers submitted to the conference from an international authorship. These papers were refereed by the Program Committee and thirty-five papers have been accepted for the conference. We would like to thank the authors of all papers which were submitted to the conference, both those whose work is included in these proceedings, and those whose work could not be accommodated.

The papers included in the conference come from a number of countries including fifteen from Australia, three each from the USA, Japan, and Germany, two each from Finland and Taiwan, and one each from Singapore, Yugoslavia, Austria, Hong Kong, Norway, Belgium, and the Czech Republic. These papers covered topics in network security, block ciphers, stream ciphers, authentication codes, software security, Boolean functions, secure electronic commerce, public key cryptography, cryptographic hardware, access control, cryptographic protocols, secret sharing, and digital signatures.

The conference included a panel session entitled "Can E-commerce be safe and secure on the Internet?". This panel was chaired by William Caelli and included leaders in technology, law, and public policy related to the issues and problems of safety and security of global electronic commerce on the Internet.

We would like to thank all the people involved in organizing this conference. In particular we would like to thank members of the program committee for their effort in reviewing papers and designing an excellent program. Special thanks to members of the organizing committee for their time and effort in organizing the conference especially Andrew Clark, Gary Gaskell, Betty Hansford, Mark Looi, and Christine Orme. Finally we would like to thank all the participants at ACISP'98.

May 1998 Colin Boyd and Ed Dawson

AUSTRALASIAN CONFERENCE ON INFORMATION SECURITY AND PRIVACY ACISP'98

Sponsored by
Information Security Research Centre, QUT, Australia
Australian Computer Society
ERACOM Pty Ltd
Media Tech Pacific Pty Ltd

General Chair:

Ed Dawson	*Queensland University of Technology, Australia*

Program Chairs:

Colin Boyd	*Queensland University of Technology, Australia*
Ed Dawson	*Queensland University of Technology, Australia*

Program Committee:

Mark Ames	*Telstra, Australia*
Bob Blakley	*Texas A&M University, USA*
William Caelli	*Queensland University of Technology, Australia*
Lyal Collins	*Commonwealth Bank, Australia*
Jovan Golić	*University of Belgrade, Yugoslavia*
Dieter Gollman	*University of London, UK*
Sokratis Katsikas	*University of the Aegean, Greece*
Wenbo Mao	*Hewlett-Packard Laboratories, UK*
Sang-Jae Moon	*Kyungpook National University, Korea*
Winfried Müller	*University of Klagenfurt, Austria*
Eiji Okamoto	*JAIST, Japan*
Josef Pieprzyk	*University of Wollongong, Australia*
Steve Roberts	*Witham Pty Ltd, Australia*
John Rogers	*Department of Defence, Australia*
Greg Rose	*QUALCOMM, Australia*
Rei Safavi-Naini	*University of Wollongong, Australia*
Eugene Spafford	*COAST, Purdue University, USA*
Stafford Tavares	*Queen's University, Canada*
Vijay Varadharajan	*University of Western Sydney, Australia*
Yuliang Zheng	*Monash University, Australia*

Table of Contents

Invited Speakers

A Review of the SESAME Development 1
Per Kaijser

The Security of Public Key Cryptosystems Based on Integer Factorization 9
Siguna Müller, Winfried B. Müller

Network Security I

A Uniform Approach to Securing Unix Applications Using SESAME 24
Paul Ashley, Mark Vandenwauver, Bradley Broom

Integrated Management of Network and Host Based Security Mechanisms . 36
Rainer Falk, Markus Trommer

Covert Distributed Computing Using Java Through Web Spoofing 48
Jeffrey Horton, Jennifer Seberry

Block Ciphers

Differential Cryptanalysis of a Block Cipher 58
Xun Yi, Kwok Yan Lam, Yongfei Han

On Private-Key Cryptosystems Based on Product Codes 68
Hung-Min Sun, Shiuh-Pyng Shieh

Key Schedules of Iterative Block Ciphers 80
Gary Carter, Ed Dawson, Lauren Nielsen

Network Security II

Low-Cost Secure Server Connection with Limited-Privilege Clients 90
Uri Blumenthal, N. C. Hien, J. H. Rooney

A Solution to Open Standard of PKI 99
Qi He, Katia Sycara, Zhongmin Su

Comparison of Commitment Schemes Used in Mix-Mediated Anonymous Communication for Preventing Pool-Mode Attacks 111
E. Franz, A. Graubner, A. Jerichow, A. Pfitzmann

Stream Ciphers

Correlation Attacks on Up/Down Cascades 123
Jovan Dj. Golić, Renato Menicocci

A Stream Cipher Based on Linear Feedback over GF(2^8) 135
Greg Rose

A Probabilistic Correlation Attack on the Shrinking Generator 147
L. Simpson, J. Dj. Golić, E. Dawson

Authentication Codes and Boolean Functions

Bounds and Constructions for A^3-code with Multi-senders 159
Rei Safavi-Naini, Yejing Wang

Rotation-Symmetric Functions and Fast Hashing 169
Josef Pieprzyk, Cheng Xin Qu

How to Improve the Nonlinearity of Bijective S-Boxes 181
William Millan

Software Security and Electronic Commerce

Object Modeling of Cryptographic Algorithms with UML 193
Rauli Kaksonen, Petri Mähönen

Adapting an Electronic Purse for Internet Payments 205
Martin Manninger, Robert Schischka

LITESET: A Light-Weight Secure Electronic Transaction Protocol 215
Goichiro Hanaoka, Yuliang Zheng, Hideki Imai

Public Key Cryptography

Applications of Linearised and Sub-linearised Polynomials to Information Security 227
Marie Henderson

Protocol Failures Related to Order of Encryption and Signature: Computation of Discrete Logarithms in RSA Groups 238
Mark Chen, Eric Hughes

Hardware

Protection Against EEPROM Modification Attacks 250
W. W. Fung, J. W. Gray, III

Trends in Quantum Cryptography in Czech Republic 261
Jaroslav Hruby

Access Control

A High Level Language for Conventional Access Control Models 273
Yun Bai, Vijay Varadharajan

Fast Access Control Decisions from Delegation Certificate Databases 284
Tuomas Aura

Meta Objects for Access Control: Role-Based Principals 296
Thomas Riechmann, Jürgen Kleinöder

A Dynamically Typed Access Control Model 308
Jonathon E. Tidswell, John M. Potter

Protocols

Efficient Identity-Based Conference Key Distribution Protocols 320
Shahrokh Saeednia, Rei Safavi-Naini

A Formal Model for Systematic Design of Key Establishment Protocols ... 332
Carsten Rudolph

Key Establishment Protocols for Secure Mobile Communications: A Selective Survey 344
Colin Boyd, Anish Mathuria

Detecting Key-Dependencies 356
Tage Stabell-Kulø, Arne Helme, Gianluca Dini

Secret Sharing

Secret Sharing in Multilevel and Compartmented Groups 367
Hossein Ghodosi, Josef Pieprzyk, Rei Safavi-Naini

On Construction of Cumulative Secret Sharing Schemes................. 379
Hossein Ghodosi, Josef Pieprzyk, Rei Safavi-Naini, Huaxiong Wang

A Comment on the Efficiency of Secret Sharing Scheme over any Finite Abelian Group 391
Yvo Desmedt, Brian King, Wataru Kishimoto, Kaoru Kurosawa

Digital Signatures

A User Identification System Using Signature Written with Mouse 403
Agus Fanar Syukri, Eiji Okamoto, Masahiro Mambo

On Zhang's Nonrepudiable Proxy Signature Schemes 415
Narn-Yih Lee, Tzonelih Hwang, Chih-Hung Wang

Author Index 423