Lecture Notes in Computer Science 3810

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Yvo G. Desmedt Huaxiong Wang
Yi Mu Yongqing Li (Eds.)

Cryptology and Network Security

4th International Conference, CANS 2005
Xiamen, China, December 14-16, 2005
Proceedings

Springer

Volume Editors

Yvo G. Desmedt
University College London, Department of Computer Science
Gower Street, London WC1E 6BT, UK
E-mail: y.desmedt@cs.ucl.ac.uk

Huaxiong Wang
Macquarie University, Department of Computing
NSW 2109, Australia
E-mail: hwang@ics.mq.edu.au

Yi Mu
University of Wollongong, School of Information Technology and Computer Science
Wollongong, NSW 2522, Australia
E-mail: ymu@uow.edu.au

Yongqing Li
Fujian Normal University, School of Mathematics and Computer Science
Fujian, Fuzhou 350007, China
E-mail: yqli@fjnu.edu.cn

Library of Congress Control Number: 2005936808

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

ISSN 0302-9743
ISBN-10 3-540-30849-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30849-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11599371 06/3142 5 4 3 2 1 0

Preface

The 4th International Conference on Cryptology and Network Security (CANS 2005) was held in Xiamen, Fujian Province, China, December 14–16, 2005. The conference was sponsored by the Fujian Normal University and Fujian Digital Certificate Authority Co. Ltd and was organized in cooperation with the International Association for Cryptologic Research (IACR).

The first International Workshop on Cryptology and Network Security was in Taipei, Taiwan, 2001. The second one was in San Francisco, California, USA, September 26–28, 2002, and the third in Miami, Florida, USA, September 24–26, 2003. CANS 2005 was the first CANS with proceedings published in the *Lecture Notes in Computer Science* series by Springer.

The Program Committee received 118 submissions, and accepted 28 papers from which 1 withdrew and thus 27 papers were included in the proceedings. The reviewing process took eight weeks, each paper was carefully evaluated by at least three members from the Program Committee. We appreciate the hard work of the members of the Program Committee and external referees who gave many hours of their valuable time. Thanks to Carl Ellison, Goce Jakimoski, Bart Preneel, Yongge Wang, Christopher Wolf and Shouhuai Xu, who acted as the shepherds of 6 papers included in the proceedings.

In addition to the contributed papers, there were two invited talks: Wenbo Mao spoke on "Research Issues in Network Security" — a practical viewpoint; and Matt Franklin on "Research Issues in Network Security" — a foundations viewpoint.

The best paper award was given to Hongbo Yu, Gaoli Wang, Guoyan Zhang and Xiaoyun Wang for their joint paper: The Second-Preimage Attack on MD4.

We would like to thank all the people involved in organizing this conference. In particular we would like to thank the Chair of the Organizing Committee, Xu Li, and people from the School of Mathematics and Computer Science, Fujian Normal University, for their time and efforts, as well as Vijayakrishnan Pasupathinathan and Qingsong Ye for their excellent work on maintaining the submission/reviewing software.

December 2005

Yvo Desmedt
Huaxiong Wang
Yi Mu
Yongqing Li

4TH International Conference on Cryptology and Network Security (CANS 2005)

Sponsored by
Fujian Normal University
Fujian Digital Certificate Authority Co. Ltd.

In Cooperation with
The International Association for Cryptologic Research (IACR)

General Chairs

Yongqing Li	Fujian Normal University, China
Yi Mu	University of Wollongong, Australia

Program Chairs

Yvo G. Desmedt	University College London, UK & Florida State Univ., USA
Huaxiong Wang	Macquarie University, Australia

Program Committee

Farooq Anjum	Telcordia, USA
Amos Beimel	Ben Gurion University, Israel
John Black	University of Colorado, USA
Carlo Blundo	University of Salerno, Italy
Jung Hee Cheon	Seoul Natl. Univ., South Korea
Cunsheng Ding	Hong Kong Univ. Sci. Tech., China
Carl Ellison	Microsoft, USA
Helena Handschuh	Gemplus, France
Thomas Johansson	University of Lund, Sweden
Antoine Joux	Université de Versailles, France
Kaoru Kurosawa	Ibaraki University, Japan
Xuejia Lai	Shanghai Jiao Tong University, China
Tanja Lange	Technical University of Denmark, Denmark
Pil Joong Lee	Pohang University, South Korea
Arjen Lenstra	Lucent, USA & Tech. Univ. Eindhoven, The Netherland
Radia Perlman	Sun Microsystems, USA
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	École Normale Supérieure, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium

C. Pandu Rangan	Indian Institute of Technology, India
Kazue Sako	NEC, Japan
Berry Schoenmakers	Tech. Univ. Eindhoven, The Netherlands
Willy Susilo	University of Wollongong, Australia
Xiaoyun Wang	Shandong Univ. Australia & Tsinghua Univ., China
Yongge Wang	University of North Carolina, USA
Duncan Wong	City University of Hong Kong, China
Susanne Wetzel	Stevens Inst. of Technology, USA
Chuan-Kun Wu	Australian Natl. Univ., Australia & SKLOIS, China
Chaoping Xing	National Univ. of Singapore, Singapore
Shouhuai Xu	University of Texas, USA
Sung-Ming Yen	National Central University, Taiwan

Organizing Committee

Li Xu (Chair)	Fujian Normal University, China
Vijayakrishnan Pasupathinathan	Macquarie University, Australia
Xuan Hui Yan	Fujian Normal University, China
Zhi Qiang Yao	Fujian Normal University, China
Qingsong Ye	Macquarie University, Australia
Sheng Yuan Zhang	Fujian Normal University, China

External Referees

Michel Abdalla
Masayuki Abe
Roberto Avanzi
Joonsang Baek
Bruno Blanchet
An Braeken
Benoit Chevallier-Mames
Kuo-Zhe Chiou
Kookrae Cho
Mathieu Ciet
Christophe Clavier
Scott Contini
Ingemar Cox
Nora Dabbous
Serge Fehr
Pierre-Alain Fouque
Chandana Gamage
Rob Granger
Goichiro Hanaoka
Swee-Huay Heng
Shoichi Hirose
Yong Ho Hwang
Sortiris Ioannidis
Goce Jakimoski
Shaoquan Jiang
Masaru Kamada
Charlie Kaufman
Tom Kevenaar
Hyungshin Kim
Seungjoo Kim
Yongdae Kim
Takeshi Koshiba
Taekyung Kwon
Heung-Kyu Lee
Jung Wook Lee
Hsi-Chung Lin
Pin Lin
Phil MacKenzie
Kengo Mori
Kathleen Moriarty
Kenny Nguyen-Qk
Svetla Nikova
M. Paramasivam
Duong Hieu Phan
Raphael C.-W. Phan
Michael Quisquater
Nicholas Sheppard
Jong Hoon Shin
Igor Shparlinski
Martijn Stam
Ron Steinfeld
Po-Chyi Su
Dongvu Tonien
Isamu Teranishi
Duong Quang Viet
Guilin Wang
Liming Wang
Enav Weinreb
Christopher Wolf
Tao Xu
Yeon Hyeong Yang
Jeong Il Yoon

Table of Contents

Cryptanalysis

The Second-Preimage Attack on MD4
Hongbo Yu, Gaoli Wang, Guoyan Zhang, Xiaoyun Wang 1

On the Security of Certificateless Signature Schemes from Asiacrypt 2003
Xinyi Huang, Willy Susilo, Yi Mu, Futai Zhang 13

On the Security of a Group Signcryption Scheme from Distributed Signcryption Scheme
Haiyong Bao, Zhenfu Cao, Haifeng Qian 26

Cryptanalysis of Two Group Key Management Protocols for Secure Multicast
Wen Tao Zhu 35

Security Analysis of Password-Authenticated Key Agreement Protocols
Kyung-Ah Shim, Seung-Hyun Seo 49

Intrusion Detection and Viruses

An Immune-Based Model for Computer Virus Detection
Tao Li, Xiaojie Liu, Hongbin Li 59

A New Model for Dynamic Intrusion Detection
Tao Li, Xiaojie Liu, Hongbin Li 72

Self Debugging Mode for Patch-Independent Nullification of Unknown Remote Process Infection
Ruo Ando, Yoshiyasu Takefuji 85

A New Unsupervised Anomaly Detection Framework for Detecting Network Attacks in Real-Time
Wei Lu, Issa Traore 96

Authentication and Signature

ID-Based Aggregate Signatures from Bilinear Pairings
Jing Xu, Zhenfeng Zhang, Dengguo Feng 110

Efficient Identity-Based Signatures and Blind Signatures
Zhenjie Huang, Kefei Chen, Yumin Wang 120

How to Authenticate Real Time Streams Using Improved Online/Offline Signatures
Chong-zhi Gao, Zheng-an Yao 134

New Authentication Scheme Based on a One-Way Hash Function and Diffie-Hellman Key Exchange
Eun-Jun Yoon, Kee-Young Yoo 147

Signcryption

Two Proxy Signcryption Schemes from Bilinear Pairings
Qin Wang, Zhenfu Cao 161

Constructing Secure Warrant-Based Proxy Signcryption Schemes
Yuan Zhou, Zhenfu Cao, Rongxing Lu 172

E-mail Security

Design and Implementation of an Inline Certified E-mail Service
Stelvio Cimato, Clemente Galdi, Raffaella Giordano, Barbara Masucci, Gildo Tomasco 186

Efficient Identity-Based Protocol for Fair Certified E-mail Delivery
Zhenfeng Zhang, Jing Xu, Dengguo Feng 200

Cryptosystems

Similar Keys of Multivariate Quadratic Public Key Cryptosystems
Yuh-Hua Hu, Lih-Chung Wang, Chun-Yen Chou, Feipei Lai 211

A Note on Signed Binary Window Algorithm for Elliptic Curve Cryptosystems
Fanyu Kong, Daxing Li 223

Constructions of Almost Resilient Functions
Pin-Hui Ke, Tai-Lin Liu, Qiao-Yan Wen 236

Privacy and Tracing

A Novel Method to Maintain Privacy in Mobile Agent Applications
Kun Peng, Ed Dawson, Juanma Gonzalez Nieto, Eiji Okamoto, Javier López 247

Non-expanding Transaction Specific Pseudonymization for IP Traffic Monitoring
Lasse Øverlier, Tønnes Brekne, André Årnes 261

Information Hiding

Revaluation of Error Correcting Coding in Watermarking Channel
Limin Gu, Yanmei Fang, Jiwu Huang 274

Firewalls, Denial of Service and DNS Security

On the Performance and Analysis of DNS Security Extensions
Reza Curtmola, Aniello Del Sorbo, Giuseppe Ateniese 288

On Securing RTP-Based Streaming Content with Firewalls
Liang Lu, Rei Safavi-Naini, Jeffrey Horton, Willy Susilo 304

Safeguard Information Infrastructure Against DDoS Attacks: Experiments and Modeling
Yang Xiang, Wanlei Zhou 320

Trust Management

Distributed Credential Chain Discovery in Trust-Management with Parameterized Roles
Xian Zhu, Shaobin Wang, Fan Hong, Junguo Liao 334

Author Index 349