Lecture Notes in Computer Science 4176

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
University of California, Los Angeles, CA, 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

Sokratis K. Katsikas Javier Lopez
Michael Backes Stefanos Gritzalis
Bart Preneel (Eds.)

Information Security

9th International Conference, ISC 2006
Samos Island, Greece, August 30 – September 2, 2006
Proceedings

Springer

Volume Editors

Sokratis K. Katsikas
University of the Aegean, Mytilene, Greece
E-mail: ska@aegean.gr

Javier Lopez
University of Malaga, Spain
E-mail: jlm@lcc.uma.es

Michael Backes
Saarland University, Saarbrücken, Germany
E-mail: backes@cs.uni-sb.de

Stefanos Gritzalis
University of the Aegean, Samos, Greece
E-mail: sgritz@aegean.gr

Bart Preneel
Katholieke Universiteit Leuven, Belgium
E-mail: bart.preneel@esat.kuleuven.be

Library of Congress Control Number: 2006931359

CR Subject Classification (1998): E.3, E.4, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-38341-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-38341-3 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

springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11836810 06/3142 5 4 3 2 1 0

Preface

This volume contains the papers presented at the 9th Information Security Conference (ISC 2006) held on Samos Island, Greece, during August 30 – September 2, 2006. The Conference was organized by the University of the Aegean, Greece.

ISC was first initiated as a workshop, ISW in Japan in 1997, ISW 1999 in Malaysia, ISW 2000 in Australia and then changed to the current name ISC when it was held in Spain in 2001 (ISC 2001). The latest conferences were held in Brazil (ISC 2002), UK (ISC 2003), USA (ISC 2004), and Singapore (ISC 2005).

ISC 2006 provided an international forum for sharing original research results and application experiences among specialists in fundamental and applied problems of information security.

In response to the Call for Papers, 188 papers were submitted. Each paper was reviewed by three members of the PC, on the basis of their significance, novelty, and technical quality. Of the papers submitted, 38 were selected for presentation, with an acceptance rate of 20%.

We would like to express our gratitude to the members of the Program Committee, as well as the external reviewers, for their constructive and insightful comments during the review process and discussion that followed. Moreover, we would like to thank all the members of the Organizing Committee for their continuous and valuable support. We also wish to express our thanks to Alfred Hofmann and his colleagues from Springer, for their co-operation and their excellent work during the publication process. Finally, we would like to thank all the people who submitted their papers to ISC 2006, including those whose submissions were not selected for publication, and all the delegates from around the world, who attended the ISC 2006 9th Information Security Conference. Without their support the conference would not have been possible.

August 2006

Sokratis K. Katsikas
Javier Lopez
Michael Backes
Stefanos Gritzalis
Bart Preneel

ISC 2006 9th Information Security Conference

General Co-chairs

Sokratis K. Katsikas	University of the Aegean, Greece
Javier Lopez	University of Malaga, Spain

Program Committee Co-chairs

Michael Backes	Saarland University, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Bart Preneel	Katholieke Universiteit Leuven, Belgium

Program Committee

A. Acquisti	Carnegie Mellon University, USA
N. Asokan	Nokia Research Center, Finland
V. Atluri	Rutgers University, USA
T. Aura	Microsoft Research, UK
F. Bao	Institute for Infocomm Research, Singapore
J. Baras	University of Maryland, USA
D. Basin	ETH Zurich, Switzerland
G. Bella	University of Catania, Italy
J. Benaloh	Microsoft Research, USA
E. Bertino	CERIAS, Purdue University, USA
A. Biryukov	University of Luxembourg, Luxembourg
M. Burmester	Florida State University, USA
S. De Capitani di Vimercati	University of Milan, Italy
D. Catalano	ENS, France
D. Chadwick	University of Kent, UK
R. Cramer	CWI and Leiden University, The Netherlands
B. Crispo	Vrije Universiteit Amsterdam, The Netherlands
G. Danezis	Katholieke Universiteit Leuven, Belgium
A. Datta	Stanford University, USA
E. Dawson	Queensland University of Technology, Australia
S. Furnell	University of Plymouth, UK
V. Gligor	University of Maryland, USA
D. Gollmann	Hamburg University of Technology, Germany
H. Handschuh	Spansion, France
D. Hofheinz	CWI, The Netherlands
D. Hutter	DFKI, Germany

J. Ioannidis	Columbia University, USA
A. Juels	RSA Laboratories, USA
T. Karygiannis	NIST, USA
S. Kokolakis	University of the Aegean, Greece
C. Lambrinoudakis	University of the Aegean, Greece
H. Lipmaa	Cybernetica AS & University of Tartu, Estonia
M. Mambo	University of Tsukuba, Japan
H. Mantel	RWTH Aachen, Germany
W. Mao	HP Labs, China
F. Massacci	University of Trento, Italy
M. Merabti	Liverpool John Moores University, UK
C. Mitchell	Royal Holloway, University of London, UK
A. Odlyzko	University of Minnesota, USA
E. Okamoto	University of Tsukuba, Japan
J. A. Onieva	University of Malaga, Spain
R. Oppliger	eSECURITY Technologies, Switzerland
G. Pernul	University of Regensburg, Germany
A. Pfitzmann	Dresden University of Technology, Germany
V. Rijmen	Graz University of Technology, Austria
P.Y.A. Ryan	University of Newcastle upon Tyne, UK
K. Sakurai	Kyushu University, Japan
P. Samarati	University of Milan, Italy
D. Serpanos	University of Patras, Greece
P. Tuyls	Philips Research and K.U. Leuven, The Netherlands and Belgium
J. Villar	Universitat Politecnica Catalunya, Spain
M. Yung	Columbia University and RSA Laboratories, USA
Y. Zheng	University of North Carolina at Charlotte, USA
J. Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Asnar, W.
Balopoulos, Theodoros
Batina, Lejla
Bergmann, Mike
Bin Abd Razak, Shukor
Cardenas, Alvaro A.
Carvounas, Christophe
Cascella, Roberto
Chen, Haibo
Clauí, Sebastian
Cremonini, Marco
Das, Tanmoy Kanti
de Medeiros, Breno
De Win, Bart
Dobmeier, Wolfgang
Doser, Juergen
Fehr, Serge
Fergus, Paul
Fernandez, Gerardo
Fouque, Pierre-Alain
Fuchs, L.
Fukushima, Kazuhide
Geneiatakis, Dimitris
Gonzalez, Juanma
Goubin, Louis
Gouget, Aline
Guajardo, Jorge

Gymnopoulos, Lazaros
Hankes Drielsma, Paul
Henricksen, Matt
Her, Yong-Sork
Herranz, Javier
Hilty, Manuel
Holmstroem, Ursula
Hori, Yoshiaki
Kambourakis, George
Karyda, Maria
Katzenbeisser, Stefan
Kiltz, Eike
Koepf, Boris
Kolter, Jan
Koshutanski, Hristo
Krausser, Tina
Kunihiro, Noboru
Kopsell, Stefan
Lano, Joseph
Lee, Soo Bum
Lindqvist, Janne
Llewellyn-Jones, David
Meckl, Norbert S.
Muschall, B.
Naccache, David
Naliuka, Katerina
Neven, Gregory
Padr, Carles
Papadaki, Maria
Peng, Kun
Qiang, Weizhong
Schillinger, Rolf
Schlaeger, Christian
Schrijen, Geert-Jan
Seys, Stefaan
Skoric, Boris
Stefanidis, Kyriakos
Steinbrecher, Sandra
Sudbrock, Henning
Taban, Gelareh
Tu, Feng
Ueshige, Yoshifumi
van Le, Tri
Vercauteren, Frederik
Vigano, Luca
Volkamer, Melanie
Westfeld, Andreas
Wolf, Christopher
Woo, Chaw-Seng
Wu, Yongdong
Yatshukin, Artsiom
Yudistira, D.
Zannone, Nicola
Zhao, Yunlei
Zhong, Xiang
Zhou, Bo
Zhou, Juxiang
Zhu, Xusong

Table of Contents

Software Security

Extending .NET Security to Unmanaged Code 1
Patrick Klinkoff, Christopher Kruegel, Engin Kirda, Giovanni Vigna

Transparent Run-Time Prevention of Format-String Attacks Via Dynamic Taint and Flexible Validation 17
Zhiqiang Lin, Nai Xia, Guole Li, Bing Mao, Li Xie

Privacy and Anonymity

Low Latency Anonymity with Mix Rings 32
Matthew Burnside, Angelos D. Keromytis

Breaking Four Mix-Related Schemes Based on Universal Re-encryption 46
George Danezis

Weak k-Anonymity: A Low-Distortion Model for Protecting Privacy 60
Maurizio Atzori

Protecting Data Privacy Through Hard-to-Reverse Negative Databases 72
Fernando Esponda, Elena S. Ackley, Paul Helman, Haixia Jia, Stephanie Forrest

Block Ciphers and Hash Functions

Related-Key Rectangle Attack on 42-Round SHACAL-2 85
Jiqiang Lu, Jongsung Kim, Nathan Keller, Orr Dunkelman

On the Collision Resistance of RIPEMD-160 101
Florian Mendel, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen

Digital Signatures

Blind Ring Signatures Secure Under the Chosen-Target-CDH Assumption 117
Javier Herranz, Fabien Laguillaumie

Multi-party Concurrent Signatures 131
Dongvu Tonien, Willy Susilo, Reihaneh Safavi-Naini

Formal Security Model of Multisignatures 146
Yuichi Komano, Kazuo Ohta, Atsushi Shimbo, Shinichi Kawamura

Cryptanalysis of Variants of UOV 161
Yuh-Hua Hu, Chun-Yen Chou, Lih-Chung Wang, Feipei Lai

Stream Ciphers

Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles 171
Christophe De Cannière

Cryptanalysis of the Bluetooth E_0 Cipher Using OBDD's 187
Yaniv Shaked, Avishai Wool

Encryption I

A Partial Key Exposure Attack on RSA Using a 2-Dimensional Lattice 203
Ellen Jochemsz, Benne de Weger

On the Integration of Public Key Data Encryption and Public Key Encryption with Keyword Search 217
Joonsang Baek, Reihaneh Safavi-Naini, Willy Susilo

Collusion-Free Policy-Based Encryption 233
Walid Bagga, Refik Molva

Pervasive Computing

Using Multiple Smart Cards for Signing Messages at Malicious Terminals 246
István Zsolt Berta

Diverging Keys in Wireless Sensor Networks 257
Michał Ren, Tanmoy Kanti Das, Jianying Zhou

Encryption II

A Generic Transformation from Symmetric to Asymmetric Broadcast Encryption 270
Ulrich Huber, Ahmad-Reza Sadeghi

Transparent Image Encryption Using Progressive JPEG 286
Thomas Stütz, Andreas Uhl

Network Security

Preserving TCP Connections Across Host Address Changes 299
Vassilis Prevelakis, Sotiris Ioannidis

A Security Architecture for Protecting LAN Interactions 311
André Zúquete, Hugo Marques

Simulation of Internet DDoS Attacks and Defense 327
Igor Kotenko, Alexander Ulanov

SNOOZE: Toward a Stateful NetwOrk prOtocol fuzZEr 343
Greg Banks, Marco Cova, Viktoria Felmetsger, Kevin Almeroth, Richard Kemmerer, Giovanni Vigna

Watermarking and DRM

Rights Protection for Data Cubes 359
Jie Guo, Yingjiu Li, Robert H. Deng, Kefei Chen

An Efficient Probabilistic Packet Marking Scheme (NOD-PPM) 373
Huifang Yin, Jun Li

Intrusion Detection and Worms

Resistance Analysis to Intruders' Evasion of Detecting Intrusion 383
Jianhua Yang, Yongzhong Zhang, Shou-Hsuan Stephen Huang

A Wireless Intrusion Detection System for Secure Clustering and Routing in Ad Hoc Networks 398
Luciano Bononi, Carlo Tacconi

Anomaly Intrusion Detection Based on Clustering a Data Stream 415
Sang-Hyun Oh, Jin-Suk Kang, Yung-Cheol Byun, Taikyeong T. Jeong, Won-Suk Lee

Robust Reactions to Potential Day-Zero Worms Through Cooperation and Validation 427
K. Anagnostakis, S. Ioannidis, A.D. Keromytis, M.B. Greenwald

Key Exchange

An Authentication and Key Exchange Protocol for Secure Credential Services 443
SeongHan Shin, Kazukuni Kobara, Hideki Imai

A Non-malleable Group Key Exchange Protocol Robust Against Active Insiders 459
Yvo Desmedt, Josef Pieprzyk, Ron Steinfeld, Huaxiong Wang

Security Protocols and Formal Methods

Formalising Receipt-Freeness 476
H.L. Jonker, E.P. de Vink

Enhancing the Security and Efficiency of 3-D Secure 489
Mohammed Assora, Ayoub Shirvani

Designing and Verifying Core Protocols for Location Privacy 502
David von Oheimb, Jorge Cuellar

Information Systems Security

Delegation in a Distributed Healthcare Context: A Survey of Current Approaches 517
Mila Katzarova, Andrew Simpson

Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness 530
Jose M Torres, Jose M Sarriegi, Javier Santos, Nicolás Serrano

Author Index 547