Lecture Notes in Computer Science 6476

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

Alfred Kobsa
University of California, Irvine, CA, 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
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max Planck Institute for Informatics, Saarbruecken, Germany

Miguel Soriano Sihan Qing
Javier Lopez (Eds.)

Information and Communications Security

12th International Conference, ICICS 2010
Barcelona, Spain, December 15-17, 2010
Proceedings

Springer

Volume Editors

Miguel Soriano
Universitat Politècnica de Catalunya, Information Security Group
Campus Nord, Jordi Girona 1-3, 08034 Barcelona, Spain
E-mail: soriano@entel.upc.edu

Sihan Qing
Chinese Academy of Sciences, Institute of Software, Beijing 100080, China
E-mail: qsihan@ss.pku.edu.cn

Javier Lopez
Universidad de Málaga, Computer Science Department
Complejo Tecnológico, Campus de Teatinos, 29071 Málaga, Spain
E-mail: jlm@lcc.uma.es

Library of Congress Control Number: 2010940207

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-17649-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-17649-4 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.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

Information and communication security must provide technological solutions to the tension between the accelerating growth of social, economical and governmental demand for digitalization of information on the one hand, and on the other, the legal and ethical obligation to protect the individuals and organizations involved.

These proceedings contain the papers accepted at the 2010 International Conference on Information and Communications Security (ICICS 2010), held in Barcelona, Spain, during December 15-17, and hosted by the Information Security Group of the Universitat Politècnica de Catalunya, UPC.

ICICS 2010 was the 12th event in the ICICS conference series, started in 1997, which brought together leading researchers and engineers involved in multiple disciplines of information and communications security, to foster the exchange of ideas in aspects including, but not limited to, authentication and authorization, distributed and mobile systems security, e-commerce, fraud control, intellectual property protection, operating system security, anonymity and privacy, and trusted computing.

In response to the call for papers, 135 submissions were received for this year's installment of the conference series. Each paper received at least three peer-reviews on the basis of its significance, novelty, technical quality and relevance to this event. The highly competitive selection process resulted in only 31 papers being accepted, subject to a final revision before publication.

ICICS 2010 was held under the sponsorship of the Spanish government and a number of private companies, particularly Scytl, which we would like to thank. More generally, we would like to express our gratitude to all those people who, in a different capacity, contributed to the realization of this event. We are indebted to the Program and Organizing Committees for their hard work in dealing with all matters related to the conference quality and organization. We are also indebted to our three invited speakers, Jianying Zhou, Grigori Kabatiansky and Bart Preneel, for graciously accepting our invitation to deliver a special talk. We would like to acknowledge the external reviewers' constructive and insightful comments during the review process.

We sincerely hope that you find these proceedings exceedingly interesting and valuable to your research.

October 2010

Javier López
Miguel Soriano
Sihan Qing

Organization

The 2010 International Conference on Information and Communications Security (ICICS 2010) was organized by the Information Security Group (ISG) of the Universitat Politècnica de Catalunya (UPC).

Program Chairs

Sihan Qing	Institute of Software, Chinese Academy of Sciences and Institute of Software and Microelectronics, Peking University, China
Miguel Soriano	Universitat Politècnica de Catalunya, Spain

General Chair

Javier López	University of Málaga, Spain

Publication Chair

Juan Hernández-Serrano	Universitat Politècnica de Catalunya, Spain

Program Committee

Mikhail Atallah	Purdue University, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Frederic Cuppens	Telecom Bretagne, France
Roberto Di Pietro	University of Roma Tre, Italy
Jesus Díaz-Verdejo	University of Granada, Spain
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia
Óscar Esparza	Universitat Politècnica de Catalunya, Spain
Praveen Gauravaram	Technical University of Denmark, Denmark
Antonio F. Gómez-Skarmeta	University of Murcia, Spain
Juan González-Nieto	Queensland University of Technology, Australia
Yong Guan	Iowa State University, USA
James Heather	University of Surrey, UK
Juan Hernández-Serrano	Universitat Politècnica de Catalunya, Spain
Chi-Sung Laih	National Cheng Kung University, Taiwan
Yingjiu Li	Singapore Management University, Singapore
Wenbo Mao	EMC, USA
Chris Mitchell	University of London, UK
Eiji Okamoto	University of Tsukuba, Japan

Carles Padró	Nanyang Technological University, Singapore
Andreas Pashalidis	K. U. Leuven, Belgium
Rodrigo Román	University of Málaga, Spain
Bimal Roy	Indian Statistical Institute, India
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	University of Milan, Italy
Ben Smyth	University of Birmingham, UK
Willy Susilo	University of Wollongong, Australia
Guilin Wang	University of Birmingham, UK
Duncan S. Wong	City University of Hong Kong, China
Wenling Wu	Institute of Software, Chinese Academy of Sciences, China
Yongdong Wu	Institute for Infocomm Research, Singapore
Jianying Zhou	Institute for Infocomm Research, Singapore

Organizing Committee

Juan Caubet, Marcel Fernández, Jordi Forné, Carlos Hernández, Olga León, Jose Moreira, Jose L. Muñoz, Esteve Pallarès, Javier Parra-Arnau, Josep Pegueroles, Jordi Puiggalí, David Rebollo-Monedero, Sergi Reñé-Vicente, Joan Tomàs-Buliart, Juan V. Vera-del-Campo

External Reviewers

Haitham Al-Sinani, Jose M. Alcaraz Calero, Juanjo Alins, Claudio Ardagna, Man Ho Au, Fabien Autrel, Samiran Bag, Josep Balasch, Roberto Battistoni, Filipe Beato, Jorge Bernal Bernabé, Sanjay Bhattacherjee, Shaoying Cai, Mauro Conti, Christopher Culnane, Nora Cuppens-Boulahia, Xiutao Feng, Marcel Fernández, Sara Foresti, Jordi Forné, Wei Gao, Joaquin Garcia-Alfaro, Pedro García-Teodoro, Manuel Gil Pérez, Felix Gómez Mármol, Choudary Gorantla, Sandra Guasch, Seda Gürses, Matt Henricksen, Xisca Hinarejos, Yoshiaki Hori, Antonio J. Jara, Qingguang Ji, Wael Kanoun, Nessim Kisserli, Ilya Kizhvatov, Tanja Lange, Gregor Leander, Olga León, Yan Li, Feng Liu, Gabriel López, Gabriel Maciá-Fernández, Luciana Marconi, Juan M. Marín Pérez, Juan A. Martínez Navarro, Jose L. Muñoz, Phong Nguyen, Ivica Nikolic, Takashi Nishide, Yanbin Pan, Javier Parra-Arnau, Gerardo Pelosi, Alejandro Pérez, Bo Qin, Hasan Qunoo, Kenneth Radke, Somindu C. Ramanna, David Rebollo-Monedero, Jason Reid, Yizhi Ren, Rafael Rodríguez, Manuel Rodríguez-Pérez, Antonio Ruiz-Martínez, F.J. Salcedo, Subhabrata Samajder, Stefan Schiffner, Chunhua Su, Juan E. Tapiador, Joan Tomás-Buliart, Elena Torroglosa, Carmela Troncoso, Juan V. Vera-del-Campo, Nino V. Verde, Kapali Viswanathan, Ralf-Philipp Weinmann, Weiping Wen, Qianhong Wu, Fubiao Xia, Zhe Xia, Jin Xu, Qiang Yan, Ziye Yang, Po-Wah Yau, Erik Zenner, Bin Zhang, Lei Zhang, Wenhui Zhang, Zongyang Zhang, Yongbin Zhou

Sponsoring Institutions

Advanced Research on Information Security and Privacy line
ARES CONSOLIDER CSD2007-00004, Spain
Scytl Secure Electronic Voting, Spain
Ministerio de Ciencia e Innovación, Spain
Department of Telematics - Universitat Politècnica de Catalunya, Spain

Table of Contents

Cryptographic Hash Functions: Theory and Practice (Invited Talk) 1
Bart Preneel

Session 1A. Access Control

Rewriting of SPARQL/Update Queries for Securing Data Access 4
Said Oulmakhzoune, Nora Cuppens-Boulahia, Frederic Cuppens, and Stephane Morucci

Fine-Grained Disclosure of Access Policies 16
Claudio Agostino Ardagna, Sabrina De Capitani di Vimercati, Sara Foresti, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, and Mario Verdicchio

Session 1B. Public Key Cryptography and Cryptanalysis

Manger's Attack Revisited 31
Falko Strenzke

Horizontal Correlation Analysis on Exponentiation 46
Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylène Roussellet, and Vincent Verneuil

Threshold Public-Key Encryption with Adaptive Security and Short Ciphertexts 62
Bo Qin, Qianhong Wu, Lei Zhang, and Josep Domingo-Ferrer

Session 1C. Security in Distributed and Mobile Systems

A Trust-Based Robust and Efficient Searching Scheme for Peer-to-Peer Networks 77
Jaydip Sen

CUDACS: Securing the Cloud with CUDA-Enabled Secure Virtualization 92
Flavio Lombardi and Roberto Di Pietro

SEIP: Simple and Efficient Integrity Protection for Open Mobile Platforms 107
Xinwen Zhang, Jean-Pierre Seifert, and Onur Acıiçmez

Securing Mobile Access in Ubiquitous Networking via Non-roaming Agreement Protocol 126
Talal Alharbi, Abdullah Almuhaideb, and Phu Dung Le

Compromise-Resilient Anti-jamming for Wireless Sensor Networks 140
Xuan Jiang, Wenhui Hu, Sencun Zhu, and Guohong Cao

Session 1D. Cryptanalysis

On Practical Second-Order Power Analysis Attacks for Block Ciphers 155
Renato Menicocci, Andrea Simonetti, Giuseppe Scotti, and Alessandro Trifiletti

Consecutive S-Box Lookups: A Timing Attack on SNOW 3G 171
Billy Bob Brumley, Risto M. Hakala, Kaisa Nyberg, and Sampo Sovio

Session 2A. Authentication

Efficient Authentication for Mobile and Pervasive Computing 186
Basel Alomair and Radha Poovendran

Security Enhancement and Modular Treatment towards Authenticated Key Exchange 203
Jiaxin Pan, Libin Wang, and Changshe Ma

Federated Secret Handshakes with Support for Revocation 218
Alessandro Sorniotti and Refik Molva

Session 2B. Fair Exchange Protocols

An Agent-Mediated Fair Exchange Protocol 235
Gerard Draper-Gil, Jianying Zhou, and Josep Lluís Ferrer-Gomila

A New Method for Formalizing Optimistic Fair Exchange Protocols 251
Ming Chen, Kaigui Wu, Jie Xu, and Pan He

Unconditionally Secure First-Price Auction Protocols Using a Multicomponent Commitment Scheme 266
Mehrdad Nojoumian and Douglas R. Stinson

Session 2C. Anonymity and Privacy

Proving Coercion-Resistance of Scantegrity II 281
Ralf Küsters, Tomasz Truderung, and Andreas Vogt

Anonymity and Verifiability in Voting: Understanding (Un)Linkability 296
Lucie Langer, Hugo Jonker, and Wolter Pieters

A Secure and Practical Approach for Providing Anonymity Protection for Trusted Platforms 311
Kurt Dietrich and Johannes Winter

Time Warp: How Time Affects Privacy in LBSs 325
Luciana Marconi, Roberto Di Pietro, Bruno Crispo, and Mauro Conti

Session 2D. Software Security

Return-Oriented Rootkit without Returns (on the x86) 340
Ping Chen, Xiao Xing, Bing Mao, and Li Xie

Experimental Threat Model Reuse with Misuse Case Diagrams 355
Jostein Jensen, Inger Anne Tøndel, and Per Håkon Meland

Automatically Generating Patch in Binary Programs Using Attribute-Based Taint Analysis 367
Kai Chen, Yifeng Lian, and Yingjun Zhang

Session 3A. Proxy Cryptosystems

Identity-Based Proxy Cryptosystems with Revocability and Hierarchical Confidentialities 383
Lihua Wang, Licheng Wang, Masahiro Mambo, and Eiji Okamoto

Ciphertext Policy Attribute-Based Proxy Re-encryption 401
Song Luo, Jianbin Hu, and Zhong Chen

Session 3B. Intrusion Detection Systems

Hybrid Detection of Application Layer Attacks Using Markov Models for Normality and Attacks 416
Rolando Salazar-Hernández and Jesús E. Díaz-Verdejo

A Trust-Based IDS for the AODV Protocol 430
Mohamed Ali Ayachi, Christophe Bidan, and Nicolas Prigent

IDS Alert Visualization and Monitoring through Heuristic Host Selection 445
Hadi Shiravi, Ali Shiravi, and Ali A. Ghorbani

A Two-Tier System for Web Attack Detection Using Linear Discriminant Method 459
Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, Wenjing Jia, and Wei-chang Yeh

Author Index 473