

*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*

Javier Lopez Gene Tsudik (Eds.)

# Applied Cryptography and Network Security

9th International Conference, ACNS 2011  
Nerja, Spain, June 7-10, 2011  
Proceedings

## Volume Editors

Javier Lopez  
University of Malaga  
Computer Science Department  
29071 Malaga, Spain  
E-mail: jlm@lcc.uma.es

Gene Tsudik  
University of California  
Computer Science Department  
Irvine, CA 92697, USA  
E-mail: gts@ics.uci.edu

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-21553-7 e-ISBN 978-3-642-21554-4  
DOI 10.1007/978-3-642-21554-4  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011928562

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

# Preface

These proceedings contain 31 papers selected for presentation at the 9th International Conference on Applied Cryptography and Network Security (ACNS 2011) held June 7-10, 2011 in Nerja (Malaga), Spain, and hosted by the Computer Science Department of the University of Malaga.

Since 2003, ACNS is an annual conference that focuses on cutting-edge advances and results in applied cryptography and systems/network security. ACNS is a forum for research of academic as well as industrial/technical nature.

This year, a total of 172 papers were submitted. They were evaluated on the basis of research significance, novelty, and technical quality. Each submission was reviewed by at least three members of the Program Committee (PC). The PC meeting was held electronically and involved intensive discussions. In the end, 31 papers were selected for presentation at the conference, corresponding to an 18% acceptance rate. A further nine papers (not included in these proceedings) were selected for the industrial track of the conference.

Many people deserve acknowledgment for having volunteered their time and energy to make ACNS 2011 a resounding success. Many thanks are due to General Co-chairs, Roberto di Pietro and Rodrigo Roman, for their valuable help with the conference organization. We are also very grateful to Cristina Alcaraz and Claudio Soriente (Publicity Co-chairs), Ersin Uzun and Pablo Najera (Web Support) and Noelia Campos (Local Organization). Clearly, we are greatly indebted to all members of the PC and external reviewers for their selfless dedication and hard work during the review and selection process. We would also like to express our appreciation to the invited/keynote speakers: Refik Molva and Ed Dawson. Last, but certainly not least, our sincere gratitude goes to all submission authors as well as to all conference attendees.

We hope that you will find the program stimulating and that it will serve as a source of inspiration for future research.

June 2011

Javier Lopez  
Gene Tsudik

**ACNS 2011**  
**9th International Conference on Applied  
Cryptography and Network Security**

Nerja (Malaga), Spain  
June 7–10, 2011

*Organized by*  
Computer Science Department  
University of Malaga  
Spain

**Program Co-chairs**

Javier Lopez  
Gene Tsudik

University of Malaga, Spain  
University of California, Irvine, USA

**General Co-chairs**

Roberto di Pietro  
Rodrigo Roman

University of Roma Tre, Italy  
University of Malaga, Spain

**Publicity Co-chairs**

Cristina Alcaraz  
Claudio Soriente

University of Malaga, Spain  
Madrid Polytechnic University, Spain

**Web Chair**

Ersin Uzun

PARC, USA

**Program Committee**

Michel Abdalla  
Elli Androulaki  
N. Asokan  
Giuseppe Ateniese

ENS, France  
Columbia University, USA  
Nokia Research, Finland  
Johns Hopkins University, USA

Alex Biryukov	University of Luxembourg, Luxembourg
Colin Boyd	Queensland University of Technology, Australia
Jan Camenisch	IBM Zurich Research, Switzerland
Jordi Castella	Universitat Rovira Virgili, Spain
Dario Catalano	Università di Catania, Italy
Liquan Chen	HP, UK
Mauro Conti	VU Amsterdam, The Netherlands
Vanesa Daza	Pompeu Fabra University, Spain
Robert Deng	Singapore Management University, Singapore
Xuhua Ding	SMU, Singapore
Karim Eldefrawy	Hughes Research Laboratory, USA
Aurelien Francillon	ETH, Switzerland
Eiichiro Fujisaki	NTT, Japan
David Galindo	University of Luxembourg, Luxembourg
Anabel Gonzalez-Tablas	UC3M, Spain
Maribel Gonzalez-Vasco	URJC, Spain
Goichiro Hanaoka	AIST, Japan
Juan Hernandez	UPC, Spain
Javier Herranz	UPC, Spain
Jaap-Henk Hoepman	Radboud University Nijmegen, The Netherlands
Sotiris Ioannidis	FORTH, Greece
Seny Kamara	Microsoft, USA
Apu Kapadia	Indiana University Bloomington, USA
Angelos D. Keromytis	Columbia University, USA
Costas Lambrinoudakis	University of Piraeus, Greece
Di Ma	University of Michigan-Dearborn, USA
Luigi Mancini	La Sapienza, Italy
Mark Manulis	TU Darmstadt and CASED, Germany
Gregorio Martinez	University of Murcia, Spain
Ivan Martinovic	TU Kaiserslautern, Germany
Refik Molva	EURECOM, France
David Naccache	ENS, France
Gabriele Oligieri	CNR, Italy
Melek Onen	EURECOM, France
Giuseppe Persiano	Università di Salerno, Italy
Kasper Rasmussen	ETH, Switzerland

Ahmad-Reza Sadeghi

Nitesh Saxena

Abdullatif Shikfa

Jessica Staddon

Angelos Stavrou

Carmela Troncoso

Serge Vaudenay

Ivan Visconti

Shouhuai Xu

Jianying Zhou

Ruhr-Universität Bochum,  
Germany

Polytechnic Institute of New York  
University, USA

Alcatel-Lucent Bell Labs, France

Google, USA

George Mason University, USA

KU Leuven, Belgium

EPFL, Switzerland

University of Salerno, Italy - UCLA,  
USA

University of Texas at San Antonio,  
USA

I2R, Singapore

## External Reviewers

Seung Geol Choi

Ang Cui

Christophe De Canniere

Sharath Hiremagalore

Ivica Nikolic

Rahul Murmura

Vasilis Pappas

Bart Preneel

Christian Rechberger

Jorge Villar

# Table of Contents

## Session 1: Malware and Intrusion Detection

Inferring Protocol State Machine from Network Traces: A Probabilistic Approach . . . . .	1
<i>Yipeng Wang, Zhibin Zhang, Danfeng (Daphne) Yao, Buyun Qu, and Li Guo</i>	
A Specification Based Intrusion Detection Framework for Mobile Phones . . . . .	19
<i>Ashwin Chaugule, Zhi Xu, and Sencun Zhu</i>	
Misuse Detection in Consent-Based Networks . . . . .	38
<i>Mansoor Alicherry and Angelos D. Keromytis</i>	

## Session 2: Attacks I

Cold Boot Key Recovery by Solving Polynomial Systems with Noise . . . .	57
<i>Martin Albrecht and Carlos Cid</i>	
Exponent Blinding Does not Always Lift (Partial) Spa Resistance to Higher-Level Security . . . . .	73
<i>Werner Schindler and Kouichi Itoh</i>	
Cryptanalysis of the Atmel Cipher in SecureMemory, CryptoMemory and CryptoRF . . . . .	91
<i>Alex Biryukov, Ilya Kizhvatov, and Bin Zhang</i>	
Cache Timing Analysis of RC4 . . . . .	110
<i>Thomas Chardin, Pierre-Alain Fouque, and Delphine Leresteux</i>	

## Session 3: Applied Crypto I

Secure Efficient Multiparty Computing of Multivariate Polynomials and Applications . . . . .	130
<i>Dana Dachman-Soled, Tal Malkin, Mariana Raykova, and Moti Yung</i>	
Private Discovery of Common Social Contacts . . . . .	147
<i>Emiliano De Cristofaro, Mark Manulis, and Bertram Poettering</i>	



## Session 4: Signatures and Friends

Sanitizable Signatures in XML Signature — Performance, Mixing Properties, and Revisiting the Property of Transparency . . . . .	166
<i>Henrich C. Pöhls, Kai Samelin, and Joachim Posegga</i>	
Double-Trapdoor Anonymous Tags for Traceable Signatures . . . . .	183
<i>Masayuki Abe, Sherman S.M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo</i>	
Hierarchical Identity-Based Chameleon Hash and Its Applications . . . . .	201
<i>Feng Bao, Robert H. Deng, Xuhua Ding, Junzuo Lai, and Yunlei Zhao</i>	

## Session 5: Eclectic Assortment

Efficient Generic Constructions of Signcryption with Insider Security in the Multi-user Setting . . . . .	220
<i>Daiki Chiba, Takahiro Matsuda, Jacob C.N. Schuldt, and Kanta Matsuura</i>	
Quantitatively Analyzing Stealthy Communication Channels . . . . .	238
<i>Patrick Butler, Kui Xu, and Danfeng (Daphne) Yao</i>	
Fully Non-interactive Onion Routing with Forward-Secrecy . . . . .	255
<i>Dario Catalano, Mario Di Raimondo, Dario Fiore, Rosario Gennaro, and Orazio Puglisi</i>	

## Session 6: Theory

Generic Fully Simulatable Adaptive Oblivious Transfer . . . . .	274
<i>Kaoru Kurosawa, Ryo Nojima, and Le Trieu Phong</i>	
Simple and Efficient Single Round Almost Perfectly Secure Message Transmission Tolerating Generalized Adversary . . . . .	292
<i>Ashish Choudhury, Kaoru Kurosawa, and Arpita Patra</i>	
Relaxed Security Notions for Signatures of Knowledge . . . . .	309
<i>Marc Fischlin and Cristina Onete</i>	

## Session 7: Encryption

LBlock: A Lightweight Block Cipher . . . . .	327
<i>Wenling Wu and Lei Zhang</i>	
On Hiding a Plaintext Length by Preencryption . . . . .	345
<i>Cihangir Tezcan and Serge Vaudenay</i>	

## Session 8: Broadcast Encryption

Fighting Pirates 2.0 .....	359
<i>Paolo D'Arco and Angel L. Perez del Pozo</i>	
Security Notions for Broadcast Encryption .....	377
<i>Duong Hieu Phan, David Pointcheval, and Mario Strefer</i>	

## Session 9: Security Services

Towards User-Friendly Credential Transfer on Open Credential Platforms .....	395
<i>Kari Kostiaainen, N. Asokan, and Alexandra Afanasyeva</i>	
Non-transferable User Certification Secure against Authority Information Leaks and Impersonation Attacks .....	413
<i>Jacob C.N. Schuldt and Goichiro Hanaoka</i>	
Composable Security Analysis of OS Services .....	431
<i>Ran Canetti, Suresh Chari, Shai Halevi, Birgit Pfizmann, Arnab Roy, Michael Steiner, and Wietse Venema</i>	

## Session 10: Attacks II

Practical Attacks on the Maelstrom-0 Compression Function .....	449
<i>Stefan Kölbl and Florian Mendel</i>	
Linear Analysis of Reduced-Round CubeHash .....	462
<i>Tomer Ashur and Orr Dunkelman</i>	
On the Indifferentiability of Fugue and Luffa .....	479
<i>Rishiraj Bhattacharyya and Avradip Mandal</i>	
Analysis of Message Injection in Stream Cipher-Based Hash Functions .....	498
<i>Yuto Nakano, Carlos Cid, Kazuhide Fukushima, and Shinsaku Kiyomoto</i>	

## Session 11: Applied Crypto II

Secure Authenticated Comparisons .....	514
<i>Keith B. Frikken, Hao Yuan, and Mikhail J. Atallah</i>	
Public-Key Encryption with Delegated Search .....	532
<i>Luan Ibraimi, Svetla Nikova, Pieter Hartel, and Willem Jonker</i>	
<b>Author Index</b> .....	551