# Lecture Notes in Computer Science 6715

Javier Lopez Gene Tsudik (Eds.)

# Applied Cryptography and Network Security

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

Springer

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

*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)

# 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 | University of Malaga, Spain |
| Gene Tsudik | University of California, Irvine, USA |

## General Co-chairs

| | |
|---|---|
| Roberto di Pietro | University of Roma Tre, Italy |
| Rodrigo Roman | University of Malaga, Spain |

## Publicity Co-chairs

| | |
|---|---|
| Cristina Alcaraz | University of Malaga, Spain |
| Claudio Soriente | Madrid Polytechnic University, Spain |

## Web Chair

| | |
|---|---|
| Ersin Uzun | PARC, USA |

## Program Committee

| | |
|---|---|
| Michel Abdalla | ENS, France |
| Elli Androulaki | Columbia University, USA |
| N. Asokan | Nokia Research, Finland |
| Giuseppe Ateniese | 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 |
| Liqun 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 Kaiserlautern, 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 | Ruhr-Universität Bochum, Germany |
| Nitesh Saxena | Polytechnic Institute of New York University, USA |
| Abdullatif Shikfa | Alcatel-Lucent Bell Labs, France |
| Jessica Staddon | Google, USA |
| Angelos Stavrou | George Mason University, USA |
| Carmela Troncoso | KU Leuven, Belgium |
| Serge Vaudenay | EPFL, Switzerland |
| Ivan Visconti | University of Salerno, Italy - UCLA, USA |
| Shouhuai Xu | University of Texas at San Antonio, USA |
| Jianying Zhou | I2R, Singapore |

## External Reviewers

Seung Geol Choi
Ang Cui
Christophe De Canniere
Sharath Hiremagalore
Ivica Nikolic
Rahul Murmuria
Vasilis Pappas
Bart Preneel
Christian Rechberger
Jorge Villar

# Table of Contents

## Session 1: Malware and Intrusion Detection

## Session 2: Attacks I

## Session 3: Applied Crypto I

## Session 4: Signatures and Friends

## Session 5: Eclectic Assortment

## Session 6: Theory

## Session 7: Encryption

## Session 8: Broadcast Encryption

## Session 9: Security Services

## Session 10: Attacks II

## Session 11: Applied Crypto II