

*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*

Claudio A. Ardagna Jianying Zhou (Eds.)

# Information Security Theory and Practice

Security and Privacy of Mobile Devices  
in Wireless Communication

5th IFIP WG 11.2 International Workshop, WISTP 2011  
Heraklion, Crete, Greece, June 1-3, 2011  
Proceedings

## Volume Editors

Claudio A. Ardagna  
Università degli Studi di Milano  
Dipartimento di Tecnologie dell'Informazione  
Via Bramante, 65, 26013 Crema (CR), Italy  
E-mail: claudio.ardagna@unimi.it

Jianying Zhou  
Institute for Infocomm Research  
1 Fusionopolis Way, #21-01 Connexis, South Tower, 138632 Singapore  
E-mail: jyzhou@i2r.a-star.edu.sg

ISSN 0302-9743  
ISBN 978-3-642-21039-6  
DOI 10.1007/978-3-642-21040-2  
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349  
e-ISBN 978-3-642-21040-2

Library of Congress Control Number: 2011927065

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© IFIP International Federation for Information Processing 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 include the papers selected for presentation at the 5th Workshop in Information Security Theory and Practice (WISTP 2011), held during June 1-3, 2011, in Heraklion, Crete, Greece.

In response to the call for papers, WISTP 2011 received 80 submissions. Each submission was evaluated on the basis of its significance, novelty, technical quality, and practical impact, and reviewed by at least three members of the Program Committee. The reviewing process was “double-blind,” that is, the identities of the reviewers and of the authors were not revealed to each other. After an intensive discussion in a two-week Program Committee meeting held electronically, 19 full papers and 8 short papers were selected for presentation at the workshop. In addition to the technical program composed of the papers in the proceedings, the workshop included three keynotes by David Naccache, Reinhard Posch, and Pim Tuyls.

WISTP 2011 was organized in cooperation with the IFIP WG 11.2 Pervasive Systems Security. This workshop was also sponsored by FORTH, Institute of Computer Science, which took care of the organization under the aegis of ENISA, and by École Normale Supérieure (ENS) and Intrinsic-ID, who provided support for the invited speakers.

There is also a long list of people who devoted their time and energy to this workshop and who deserve acknowledgment. Thanks to all the members of the Program Committee, and the external reviewers, for all their hard work in reviewing the papers. We also gratefully acknowledge all the people involved in the organization process: the WISTP Steering Committee, and Damien Sauveron and Kostantinos Markantonakis in particular, for their advice; the General Chairs, Ioannis G. Askoxylakis and Demosthenes Ikononou, for their support in the workshop organization; Cheng-Kang Chu and Sara Foresti, for their activity as Publicity Chairs. A special thanks to the three invited speakers for accepting our invitation and delivering invited talks at the workshop.

Last but certainly not least, our thanks are due to the authors for submitting the best results of their research to WISTP 2011 and to all the attendees. We hope you find the proceedings helpful for your future research activities.

June 2011

Claudio A. Ardagna  
Jianying Zhou

# Organization

The 5th Workshop in Information Security Theory and Practice (WISTP 2011) was held in Heraklion, Crete, Greece, June 1-3, 2011

## General Chairs

Ioannis G. Askoxylakis	FORTH-ICS, Greece
Demosthenes Ikonomou	ENISA, Greece

## Program Chairs

Jianying Zhou	Institute for Infocomm Research, Singapore
Claudio A. Ardagna	Università degli Studi di Milano, Italy

## Workshop/Panel/Tutorial Chair

Damien Sauveron	University of Limoges, France
-----------------	-------------------------------

## Publicity Chairs

Cheng-Kang Chu	Institute for Infocomm Research, Singapore
Sara Foresti	Università degli Studi di Milano, Italy

## Steering Committee

Angelos Bilas	FORTH-ICS and University of Crete, Greece
Konstantinos Markantonakis	Royal Holloway University of London, UK
Jean-Jacques Quisquater	Catholic University of Louvain, Belgium
Pierangela Samarati	Università degli Studi di Milano, Italy
Damien Sauveron	University of Limoges, France
Michael Tunstall	University of Bristol, UK

## Local Organizing Committee

Theodosia Bitzou	FORTH-ICS, Greece
Alison Manganas	FORTH-ICS, Greece
Nikolaos Petroulakis	FORTH-ICS, Greece (Chair)

## Program Committee

Rafael Accorsi	University of Freiburg, Germany
Vijay Atluri	Rutgers University, USA
Angelos Bilas	FORTH-ICS and University of Crete, Greece
Carlo Blundo	University of Salerno, Italy
Marco Casassa Mont	HP Labs, UK
Cheng-Kang Chu	Institute for Infocomm Research, Singapore
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Xuhua Ding	Singapore Management University, Singapore
Josep Lluís Ferrer-Gomila	Universidad de las Islas Baleares, Spain
Sara Foresti	Università degli Studi di Milano, Italy
Bok-Min Goi	Universiti Tunku Abdul Rahman, Malaysia
Stefanos Gritzalis	University of the Aegean, Greece
Guofei Gu	Texas A&M University, USA
Jaap-Henk Hoepman	TNO and Radboud University Nijmegen, The Netherlands
Yih-Chun Hu	University of Illinois, USA
Michael Huth	Imperial College London, UK
Hongxia Jin	IBM Almaden Research Center, USA
Sokratis Katsikas	University of Piraeus, Greece
Mirosław Kutylowski	Wrocław University of Technology, Poland
Jin Kwak	Soonchunhyang University, Korea
Costas Lambrinoudakis	University of the Aegean, Greece
Peng Liu	Pennsylvania State University, USA
Javier López	University of Málaga, Spain
Wenjing Lou	Worcester Polytechnic Institute, USA
Mark Manulis	Technische Universität Darmstadt, Germany
Fabio Martinelli	IIT-CNR, Italy
Carlos Maziero	Pontifical Catholic University, Brazil
Chris Mitchell	Royal Holloway University of London, UK
Katerina Mitrokotsa	EPFL, Switzerland
Jose Onieva	University of Málaga, Spain
Ferruh Ozbudak	Middle East Technical University, Turkey
Stefano Paraboschi	University of Bergamo, Italy
Gerardo Pelosi	University of Bergamo, Italy
Raphael Phan	Loughborough University, UK
Joachim Posegga	University of Passau, Germany
Jean-Jacques Quisquater	Catholic University of Louvain, Belgium
Jason Reid	Queensland University of Technology, Australia
Kui Ren	Illinois Institute of Technology, USA

Reihaneh Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Gokay Saldamli	Bogazici University, Turkey
Pierangela Samarati	Università degli Studi di Milano, Italy
Jose Maria Sierra	Carlos III University of Madrid, Spain
Miguel Soriano	Technical University of Catalonia, Spain
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Kyushu University, Japan
Michael Tunstall	University of Bristol, UK
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Jian Weng	Jinan University, China
Chan Yeob Yeun	Khalifa University of Science, Technology and Research, UAE
Heung-Youl Youm	Soonchunhyang University, Korea

## External Reviewers

Isaac Agudo	Fengjun Li
Cristina Alcaraz	Ming Li
lessandro Barenghi	Yang Li
Lejla Batina	Bisheng Liu
Jung Hee Cheon	Jian Liu
Jihyuk Choi	Peng Liu
Sherman S.M. Chow	Hans Löhr
Gabriele Costa	Changshe Ma
Giampiero Costantino	Bilgin Metin
Eleni Darra	Alexander Meurer
Isao Echizen	Berna Ors
Dominik Engel	Pedro Peris-Lopez
Carmen Fernandez-Gago	Jing Qin
Kazuhide Fukushima	Panagiotis Rizomiliotis
Dimitris Geneiatakis	Rodrigo Roman
Johann Großschädl	Nashad Safa
Dongguk Han	Daniel Schreckling
Takuya Hayashi	Daniele Sgandurra
Luca Henzen	Zafar Shahid
Yoshiaki Hori	Thomas Stocker
Vincenzo Iovino	Donghai Tian
Keiichi Iwamura	Aggeliki Tsohou
Christos Kalloniatas	Nikos Vrakas
Markus Karwe	Witold Waligora
Young-Sik Kim	Jie Wang
Lukasz Krzywiecki	Pengwei Wang
Przemyslaw Kubiak	Kok-Sheik Wong
Hoi Le	Claus Wonnemann

Chao Yang  
Yanjiang Yang  
Artsiom Yautsiukhin

Ilsun You  
Jialong Zhang  
Wen Tao Zhu

## **Sponsoring Institutions**

IFIP WG11.2 Pervasive Systems Security  
FORTH, Institute of Computer Science, Greece  
European Network and Information Security Agency (ENISA), Greece  
École Normale Supérieure (ENS), France  
Intrinsic-ID, The Netherlands



# Table of Contents

## Keynote Speech

Can Code Polymorphism Limit Information Leakage? .....	1
<i>Antoine Amarilli, Sascha Müller, David Naccache, Daniel Page, Pablo Rauzy, and Michael Tunstall</i>	

## Mobile Authentication and Access Control

Mobile Electronic Identity: Securing Payment on Mobile Phones .....	22
<i>Chen Bangdao and A.W. Roscoe</i>	
Role-Based Secure Inter-operation and Resource Usage Management in Mobile Grid Systems .....	38
<i>Antonios Gouglidis and Ioannis Mavridis</i>	

## Lightweight Authentication

SSL/TLS Session-Aware User Authentication Using a GAA Bootstrapped Key .....	54
<i>Chunhua Chen, Chris J. Mitchell, and Shaohua Tang</i>	
An Almost-Optimal Forward-Private RFID Mutual Authentication Protocol with Tag Control .....	69
<i>Paolo D'Arco</i>	
Affiliation-Hiding Authentication with Minimal Bandwidth Consumption .....	85
<i>Mark Manulis and Bertram Poettering</i>	

## Algorithms

Formal Framework for the Evaluation of Waveform Resynchronization Algorithms .....	100
<i>Sylvain Guilley, Karim Khalfallah, Victor Lomne, and Jean-Luc Danger</i>	
Solving DLP with Auxiliary Input over an Elliptic Curve Used in TinyTate Library .....	116
<i>Yumi Sakemi, Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda</i>	
Information Leakage Discovery Techniques to Enhance Secure Chip Design .....	128
<i>Alessandro Barenghi, Gerardo Pelosi, and Yannick Tégli</i>	

## Hardware Implementation

A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES Like Sardines . . . . .	144
<i>Michael Hutter, Martin Feldhofer, and Johannes Wolkerstorfer</i>	
An Evaluation of Hash Functions on a Power Analysis Resistant Processor Architecture . . . . .	160
<i>Simon Hoerder, Marcin Wójcik, Stefan Tillich, and Daniel Page</i>	
A Comparison of Post-Processing Techniques for Biased Random Number Generators . . . . .	175
<i>Siew-Hwee Kwok, Yen-Ling Ee, Guanhan Chew, Kanghong Zheng, Khoongming Khoo, and Chik-How Tan</i>	

## Security and Cryptography

AES Variants Secure against Related-Key Differential and Boomerang Attacks . . . . .	191
<i>Jiali Choy, Aileen Zhang, Khoongming Khoo, Matt Henricksen, and Axel Poschmann</i>	
Leakage Squeezing Countermeasure against High-Order Attacks . . . . .	208
<i>Housseem Maghrebi, Sylvain Guilley, and Jean-Luc Danger</i>	

## Security Attacks and Measures (Short Papers)

Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault . . . . .	224
<i>Michael Tunstall, Debdeep Mukhopadhyay, and Subidh Ali</i>	
Entropy of Selectively Encrypted Strings . . . . .	234
<i>Reine Lundin and Stefan Lindskog</i>	
Practical Attacks on HB and HB+ Protocols . . . . .	244
<i>Zbigniew Gołębiewski, Krzysztof Majcher, Filip Zagórski, and Marcin Zawada</i>	
Attacks on a Lightweight Mutual Authentication Protocol under EPC C-1 G-2 Standard . . . . .	254
<i>Mohammad Hassan Habibi, Mahdi R. Alagheband, and Mohammad Reza Aref</i>	

## Security Attacks

A SMS-Based Mobile Botnet Using Flooding Algorithm . . . . .	264
<i>Jingyu Hua and Kouichi Sakurai</i>	

FIRE: Fault Injection for Reverse Engineering . . . . .	280
<i>Manuel San Pedro, Mate Soos, and Sylvain Guilley</i>	

Hardware Trojan Side-Channels Based on Physical Unclonable Functions . . . . .	294
<i>Zheng Gong and Marc X. Makkes</i>	

## Security and Trust

Formal Analysis of Security Metrics and Risk . . . . .	304
<i>Leavid Krautsevich, Fabio Martinelli, and Artsiom Yautsiukhin</i>	

STORM - Collaborative Security Management Environment . . . . .	320
<i>Theodoros Ntouskas, George Pentafronimos, and Spyros Papastergiou</i>	

Trust Agreement in Wireless Mesh Networks . . . . .	336
<i>Andreas Noack</i>	

## Mobile Application Security and Privacy (Short Papers)

Secure E-Auction for Mobile Users with Low-Capability Devices in Wireless Network . . . . .	351
<i>Kun Peng</i>	

Privacy Respecting Targeted Advertising for Social Networks . . . . .	361
<i>Christian Kahl, Stephen Crane, Markus Tschersich, and Kai Rannenber</i>	

Privacy Protection for Smartphones: An Ontology-Based Firewall . . . . .	371
<i>Johann Vincent, Christine Porquet, Maroua Borsali, and Harold Leboulanger</i>	

A Study on the Security, the Performance and the Penetration of Wi-Fi Networks in a Greek Urban Area . . . . .	381
<i>Savvas Mousionis, Alex Vakaloudis, and Constantinos Hilar</i>	

<b>Author Index</b> . . . . .	391
-------------------------------	-----