Preface

The 13th Information Security Conference (ISC 2010) was held at Deerfield Beach / Boca Raton, Florida, USA, during October 25–28, 2010. The conference was hosted by the Center for Cryptology and Information Security (CCIS) at the Mathematical Sciences Department of Florida Atlantic University in Boca Raton, Florida.

ISC is an annual international conference covering research in theory and applications of information security and aims to attract high quality-papers in all technical aspects of information security as well as to provide a forum for professionals from academia and industry to present their work and exchange ideas. We are very pleased with both the number and high quality of this year’s submissions. The Program Committee received 117 submissions, and accepted 25 as full papers (acceptance rate 21%). The papers were selected after an extensive and careful refereeing process in which each paper was reviewed by at least three members of the Program Committee. A further 11 articles were selected as short papers because of their appropriateness and high quality. A new experimental format was adopted this year: pre-conference proceedings of all accepted papers were made available at the conference. This provided an additional opportunity for authors to solicit and obtain early feedback. The Springer proceedings were mailed to the authors after the conference.

Many people deserve our gratitude for their generous contributions to the success of this conference. We wish to thank all the members of the ISC 2010 Program Committee, as well as the external reviewers, for reviewing, deliberating and selecting (under severe time pressure and in the middle of summer) an excellent set of papers. Thanks are also due to Masahiro Mambo who, as our contact person on the ISC Steering Committee, helped maintain ISC traditions and provided guidance. Mega-kudos to Ivana Ilić for contributing a tremendous amount of work, much of it beyond the call of duty. Also, a great deal of thanks are due to: Emily Cimillo for helping with budgetary issues, Leanne Magliveras for keeping track of numerous organizational tasks, as well as Nidhi Singhi, Nikhil Singhi and Nicola Pace for invaluable assistance with various conference aspects.

We are delighted to acknowledge the sponsorship of CCIS; of the Center for Security and Assurance in IT (C-SAIT) of Florida State University; of the Charles E. Schmidt College of Science at Florida Atlantic University; and of the DATAMAXX group, the latter having provided support for the Best Student Paper Awards and additional funds for graduate student support.
Last but not least, on behalf of all those involved in organizing the conference we would like to thank all the authors who submitted papers to this conference. Without their submissions and support, ISC could not have been a success.

November 2010

Spyros Magliveras
Mike Burmester
Gene Tsudik
Organization

General Chair

Spyros Magliveras  CCIS, Florida, USA

Program Committee Co-chairs

Mike Burmester  Florida State University, USA
Gene Tsudik  University of California, Irvine, USA

Program Committee

Giuseppe Ateniese  Johns Hopkins University, USA
Elisa Bertino  Purdue University, USA
Simon Blackburn  Royal Holloway, UK
Ian Blake  University of Toronto, Canada
Marina Blanton  University of Notre Dame, USA
Carlo Blundo  Università di Salerno, Italy
Colin Boyd  Queensland University of Technology Australia
Levente Buttyan  Budapest University of Technology and Economics, Hungary
Cafer Caliskan  Michigan Technical University Michigan, USA
Claude Castelluccia  INRIA, France
David Chadwick  University of Kent, UK
Jung Hee Cheon  Seoul National University, Korea
Emiliano De Cristofaro  University of California, Irvine, USA
Vanesa Daza  Universitat Pompeu Fabra, Spain
Claudia Diaz  KU Leuven, Belgium
Roberto Di Pietro  Roma Tre University, Italy
Xuhua Ding  Singapore Management University, Singapore
Wenliang Du  Syracuse University, France
Thomas Eisenbarth  CCIS, Florida, USA
Eduardo Fernandez  Florida Atlantic University, USA
Juan Garay  ATT Research, USA
Madeline Gonzalez  Cybernetica AS, Estonia
Nick Hopper  University of Minnesota, USA
Ivana Ilić  CCIS, Florida, USA
Kwangjo Kim
KAIST, Korea

Yongdae Kim
University of Minnesota, USA

Panos Kotzanikolaou
University of Piraeus, Greece

Feifei Li
Florida State University, Florida, USA

Javier Lopez
University of Malaga, Spain

Di Ma
University of Michigan, Dearborn, USA

Masahiro Mambo
University of Tsukuba, Japan

Emmanouil Magkos
University of the Ionian, Greece

Mark Manulis
TU Darmstadt, Germany

Ken Matheis
CCIS, Florida, USA

Nasir Memon
New York Polytechnic, New York, USA

Alfred Menezes
University of Waterloo, Canada

Ron Mullin
University of Waterloo, Canada

Jorge Munilla
Universidad de Málaga, Spain

David Naccache
ENS and Université Paris II, France

Juan Gonzalez Nieto
Queensland University of Technology
Australia

Rei Safavi-Naini
University of Calgary, Canada

Pierangela Samarati
Università degli Studi di Milano, Italy

Nitesh Saxena
CS Dept, Polytechnic Institute of NYU
USA

Elaine Shi
PARC, USA

Radu Sion
Stony Brook University, USA

Nikhil Singh
CCIS, Florida, USA

Nidhi Singhi
CCIS, Florida, USA

Claudio Soriente
Madrid Polytechnic, Spain

Michal Sramka
Universitat Rovira i Virgili, Spain

Rainer Steinwandt
CCIS, Florida, USA

Doug Stinson
University of Waterloo, Canada

Jonathan Trostle
Johns Hopkins University, USA

Patrick Traynor
Georgia Institute of Technology, USA

Tran van Trung
University of Essen-Duisburg, Germany

Ivan Visconti
Università di Salerno, Italy

Bogdan Warinschi
University of Bristol, UK

Shouhuai Xu
University of Texas at San Antonio
USA

Sencun Zhu
Pennsylvania State University, USA
External Reviewers

Gegerly Acs          Claudio A. Ardagna
Andrey Bogdanov     Eric Chan-Tin
Sanjit Chatterjee   Andrew Clark
Mauro Conti         Sabrina De Capitani di Vimercati
Elke De Mulder      Carmen Fernandez
Sara Foresti        Aurelien Francillon
Tim Gueneysu        Tzipora Halevi
Darrel Hankerson    Kristiyan Haralambiev
Jens Hermans        Javier Herranz
Seokhie Hong        Sebastiaan Indesteege
Vincenzo Iovino     Rob Jansen
Yoonchan Jhi        Seny Kamara
B. Hoon Kang        Jaeheon Kim
Jihye Kim           Taekyoung Kwon
Kerstin Lemke-Rust  Zi Lin
Gabriel Maganis     Joan Mir
Amir Moradi         Jose Morales
Francisco Moyano    Arvind Narayanan
Yuan Niu            Jose A. Onieva
Andrs Ortiz         Abhi Pandya
Sai Teja Peddinti   Daniele Perito
Benny Pinkas        Alessandra Scafuro
Stefan Schiffner    Max Schuchard
Gautham Sekar       Jae Hong Seo
Douglas Stebila     Dongdong Sun
Germm Sez           Anthony Van Herrewege
Nino V. Verde       Jose L. Vivas
Jonathan Voris      Qianhong Wu
Wei Xu              Li Xu
Aaram Yun           Zhenxin Zhan
Lei Zhang
Table of Contents

Attacks and Analysis

Improved Collision Attacks on the Reduced-Round Grøstl Hash Function ........................................................ 1
   Kota Ideguchi, Elmar Tischhauser, and Bart Preneel

Improved Distinguishing Attack on Rabbit ......................... 17
   Yi Lu and Yvo Desmedt

Cryptanalysis of the Convex Hull Click Human Identification Protocol ......................................................... 24
   Hassan Jameel Asghar, Shujun Li, Josef Pieprzyk, and Huaxiong Wang

An Analysis of DepenDNS ............................................. 31
   Nadhem J. AlFardan and Kenneth G. Paterson

Analysis

Security Reductions of the Second Round SHA-3 Candidates .......... 39
   Elena Andreeva, Bart Mennink, and Bart Preneel

Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents ............... 54
   Özgür Dagdelen and Marc Fischlin

Revisiting the Security of the ALRED Design ..................... 69
   Marcos A. Simplicio Jr., Paulo S.L.M. Barreto, and Tereza C.M.B. Carvalho

Authentication, PIR and Content Identification

Lightweight Anonymous Authentication with TLS and DAA for Embedded Mobile Devices .................................. 84
   Christian Wachsmann, Liqun Chen, Kurt Dietrich, Hans Löhr, Ahmad-Reza Sadeghi, and Johannes Winter

Implicit Authentication through Learning User Behavior .......... 99
   Elaine Shi, Yuan Niu, Markus Jakobsson, and Richard Chow
Efficient Computationally Private Information Retrieval from Anonymity or Trapdoor Groups ................................................. 114
Jonathan Trostle and Andy Parrish

Video Streaming Forensic – Content Identification with Traffic Snooping ................................................................. 129
Yali Liu, Ahmad-Reza Sadeghi, Dipak Ghosal, and Biswanath Mukherjee

Privacy

Fair and Privacy-Preserving Multi-party Protocols for Reconciling Ordered Input Sets ................................................................ 136
Georg Neugebauer, Ulrike Meyer, and Susanne Wetzel

Enhancing Security and Privacy in Certified Mail Systems Using Trust Domain Separation .................................................. 152
Arne Tauber and Thomas Rössler

Privacy-Preserving ECC-Based Grouping Proofs for RFID .............. 159
Lejla Batina, Yong Ki Lee, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede

Malware, Crimeware and Code Injection

Artificial Malware Immunization Based on Dynamically Assigned Sense of Self ................................................................. 166
Xinyuan Wang and Xuxian Jiang

Misleading Malware Similarities Analysis by Automatic Data Structure Obfuscation ............................................................. 181
Zhi Xin, Huiyu Chen, Hao Han, Bing Mao, and Li Xie

Crimeware Swindling without Virtual Machines ........................................... 196
Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis

An Architecture for Enforcing JavaScript Randomization in Web2.0 Applications .................................................................. 203
Elias Athanasopoulos, Antonis Krithinakis, and Evangelos P. Markatos

Intrusion Detection

Summary-Invisible Networking: Techniques and Defenses .............. 210
Lei Wei, Michael K. Reiter, and Ketan Mayer-Patel

Selective Regular Expression Matching ........................................... 226
Natalia Stakhanova, Hanli Ren, and Ali A. Ghorbani
Traceability of Executable Codes Using Neural Networks .......................... 241  
*Davidson R. Boccardo, Tiago M. Nascimento, Raphael C. Machado,*  
*Charles B. Prado, and Luiz F.R.C. Carmo*

**Side Channels**

On Side-Channel Resistant Block Cipher Usage ............................... 254  
*Jorge Guajardo and Bart Mennink*

Security Implications of Crosstalk in Switching CMOS Gates .......... 269  
*Geir Olav Dyrkolbotn, Knut Wold, and Einar Snekkenes*

On Privacy Leakage through Silence Suppression ............................ 276  
*Ye Zhu*

**Cryptography**

One-Time Trapdoor One-Way Functions ...................................... 283  
*Julien Cathalo and Christophe Petit*

Public Key Encryption Schemes with Bounded CCA Security and  
Optimal Ciphertext Length Based on the CDH Assumption ................ 299  
*Mayana Pereira, Rafael Dowsley, Goichiro Hanaoka, and*  
*Anderson C.A. Nascimento*

A Short Signature Scheme from the RSA Family ......................... 307  
*Ping Yu and Rui Xue*

Efficient Message Space Extension for Automorphic Signatures ......... 319  
*Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo*

**Smartphones**

CRePE: Context-Related Policy Enforcement for Android .............. 331  
*Mauro Conti, Vu Thien Nga Nguyen, and Bruno Crispo*

Privilege Escalation Attacks on Android ................................. 346  
*Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, and*  
*Marcel Winandy*

**Biometrics**

Walk the Walk: Attacking Gait Biometrics by Imitation ............ 361  
*Bendik B. Mjaaland, Patrick Bours, and Danilo Gligoroski*
Cryptography, Application

Efficient Multiplicative Homomorphic E-Voting .......................... 381
   Kun Peng and Feng Bao

Double Spending Protection for E-Cash Based on Risk Management..... 394
   Patricia Everaere, Isabelle Simplot-Ryl, and Issa Traoré

Buffer Overflow

Integrating Offline Analysis and Online Protection to Defeat Buffer
Overflow Attacks ............................................................ 409
   Donghai Tian, Xi Xiong, Changzhen Hu, and Peng Liu

Cryptography, Theory

Deciding Recognizability under Dolev-Yao Intruder Model ............ 416
   Zhiwei Li and Weichao Wang

Indifferentiable Security Reconsidered: Role of Scheduling .......... 430
   Kazuki Yoneyama

Author Index ................................................................. 445