

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

Dimitris Gritzalis Bart Preneel
Marianthi Theoharidou (Eds.)

Computer Security – ESORICS 2010

15th European Symposium on Research in Computer Security
Athens, Greece, September 20-22, 2010
Proceedings

Volume Editors

Dimitris Gritzalis

Marianthi Theoharidou

Athens University of Economics and Business

Information Security and Critical Infrastructure Protection Research Group

Department of Informatics

76 Patission Ave., Athens, 10434, Greece

E-mail: {dgrit, mtheohar}@aueb.gr

Bart Preneel

Katholieke Universiteit Leuven

Department of Electrical Engineering-ESAT/COSIC

Kasteelpark Arenberg 10, Bus 2446, 3001 Leuven, Belgium

E-mail: bart.preneel@esat.kuleuven.be

Library of Congress Control Number: 2010933238

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-15496-4 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-15496-6 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

The European Symposium on Research in Computer Security (ESORICS) has a tradition that goes back two decades. It tries to bring together the international research community in a top-quality event that covers all the areas of computer security, ranging from theory to applications.

ESORICS 2010 was the 15th edition of the event. It was held in Athens, Greece, September 20-22, 2010. The conference received 201 submissions. The papers went through a careful review process. In a first round, each paper received three independent reviews. For the majority of the papers an electronic discussion was also organized to arrive at the final decision. As a result of the review process, 42 papers were selected for the final program, resulting in an acceptance rate of as low as 21%. The authors of accepted papers were requested to revise their papers, based on the comments received. The program was completed with an invited talk by Udo Helmbrecht, Executive Director of ENISA (European Network and Information Security Agency).

ESORICS 2010 was organized under the aegis of three Ministries of the Government of Greece, namely: (a) the Ministry of Infrastructure, Transport, and Networks, (b) the General Secretariat for Information Systems of the Ministry of Economy and Finance, and (c) the General Secretariat for e-Governance of the Ministry of Interior, Decentralization, and e-Government.

First and foremost, we would like to thank the members of the Program Committee for their extensive efforts both during the review and the discussion phase. Our task would not have been feasible without their collective knowledge and wisdom. We would also like to express our thanks to the numerous external reviewers for their contributions.

We are indebted to Sokratis Katsikas—our General Chair—for his kind encouragement, as well as to Nikos Kyrloglou—our Organizing Committee Co-chair—for his continuous support. Our appreciation goes to Triaena Tours & Congress S.A., our local organizer and official travel agent, for our fruitful co-operation.

Last, but not least, we are sincerely grateful to our sponsor, Vodafone S.A., as well as to our supporters (in alphabetical order) Adacom S.A., Encode S.A., Ernst & Young S.A., Quality & Reliability S.A., and Unisystems S.A. for their kind and generous support.

Finally, we would like to thank the submitters, authors, presenters, and participants who, all together, made ESORICS 2010 a great success.

We hope that the papers in this volume can help you with your research and professional activities, and serve as a source of inspiration during the difficult but fascinating route towards an on-line world with adequate security.

September 2010

Dimitris Gritzalis
Bart Preneel
Marianthi Theoharidou

Organization

General Chair

Sokratis Katsikas University of Piraeus (Greece)

Program Committee Chairs

Dimitris Gritzalis Athens University of Economics and Business
(Greece)
Bart Preneel K. U. Leuven (Belgium)

Organizing Committee Chairs

Nikolaos Kyrloglou Athens Chamber of Commerce and Industry
(Greece)
Marianthi Theoharidou Athens University of Economics and Business
(Greece)

Publicity Chair

Sara Foresti Università degli Studi di Milano (Italy)

Program Committee

Vijay Atluri	Rutgers University (USA)
Michael Backes	Saarland University and MPI-SWS (Germany)
Feng Bao	Institute for Infocomm Research (Singapore)
Joachim Biskup	University of Dortmund (Germany)
Carlo Blundo	Università di Salerno (Italy)
Xavier Boyen	Stanford University (USA)
Jan Camenisch	IBM Research Zurich (Switzerland)
Srdjan Capkun	ETH Zurich (Switzerland)
Richard Clayton	Cambridge University (UK)
Véronique Cortie	LORIA-CNRS (France)
Frédéric Cuppens	TELECOM Bretagne (France)
George Danezis	Microsoft Research (UK)
Sabrina de Capitani di Vimercati	Università degli Studi di Milano (Italy)
Claudia Diaz	K.U. Leuven (Belgium)
Simon Foley	University College Cork (Ireland)
Cédric Fournet	Microsoft Research (UK)

Deborah Frincke	Pacific Northwest National Laboratory (USA)
Dieter Gollmann	Hamburg University of Technology (Germany)
Thorsten Holz	Vienna University of Technology (Austria)
Bart Jacobs	University of Nijmegen (The Netherlands)
Sushil Jajodia	George Mason University (USA)
Tom Karygiannis	NIST (USA)
Stefan Katzenbeisser	T.U. Darmstadt (Germany)
Dogan Kesdogan	University of Siegen (Germany)
Aggelos Kiayias	University of Athens (Greece)
Michiharu Kudo	IBM Tokyo Research Laboratory (Japan)
Klaus Kursawe	Philips Research (The Netherlands)
Costas Lambrinoudakis	University of Piraeus (Greece)
Wenke Lee	Georgia Institute of Technology (USA)
Javier Lopez	University of Malaga (Spain)
Ioannis Mavridis	University of Macedonia (Greece)
Chris Mitchell	University of London (UK)
John Mitchell	Stanford University (USA)
Radia Perlman	Intel Corporation (USA)
Andreas Pfitzmann	T.U. Dresden (Germany)
Benny Pinkas	University of Haifa (Israel)
Michael Reiter	University of North Carolina (USA)
Peter Ryan	University of Luxembourg (Luxembourg)
Rei Safavi-Naini	University of Calgary (Canada)
Pierangela Samarati	Università degli studi Milano (Italy)
Einar Snekenes	Gjovik University College (Norway)
George Spanoudakis	City University London (UK)
Ioannis Stamatiou	University of Ioannina (Greece)
Paul Syverson	Naval Research Laboratory (USA)
Bill Tsoumas	Athens University of Economics and Business (Greece)
Michael Waidner	IBM T.J. Watson Research Center (USA)
Dirk Westhoff	HAW Hamburg (Germany)

Additional Reviewers

Agudo, Isaac	Brinkman, Richard	Clauß, Sebastian
Ahmadi, Hadi	Buttyan, Levente	Cuppens-Boulahia, Nora
Alcaraz, Cristina	Chada, Rohit	D' Arco, Paolo
Anderson, Jonathan	Chadha, Rohit	De Caro, Angelo
Autrel, Fabien	Chan, Haowen	Deursen, van, Ton
Barati, Masoud	Chase, Melissa	Dobias, Jaromir
Batina, Lejla	Chen, Liqun	Doets, Peter Jan
Ben Ghorbel, Meriam	Chenette, Nathan	Dritsas, Stelios
Bonneau, Joseph	Clarkson, Michael	Drogkaris, Prokopis

Fan, Junfeng
 Fernandez-Gago,
 Carmen
 Fitzgerald, William
 Gagne, Marin
 Galindo, David
 Garcia, Flavio
 Garcia-Alfaro, Joaquin
 Geneiataakis, Dimitris
 Gierlichs, Benedikt
 Gougolidis, Antonios
 Gregoire, Benjamin
 Hartog, den, Jerry
 Hermans, Jens
 Hoepman, Jaap-Henk
 Hoffman, Johannes
 Iovino, Vincenzo
 Jarrous, Ayman
 Jonker, Hugo
 Köpsell, Stefan
 Kellermann, Benjamin
 Kirchner, Matthias
 Konstantinou, Elisavet
 Kontogiannis, Spyros

Laud, Peeter
 Leh, Hoi
 Li, Jiangtao
 Li, Peng
 Lochner, Jan Hendrik
 Maes, Roel
 Maffei, Matteo
 Meier, Michael
 Moran, Tal
 Mostowski, Wojciech
 Murdoch, Steven
 Najera, Pablo
 Narayan,
 Shivaramakrishnan
 Nastou, Panayiotis
 Nieto, Ana
 Onieva, Jose A.
 Oostendorp, Thom
 Papagiannakopoulos,
 Panagiotis
 Paskin-Cherniavsky,
 Anat
 Poll, Erik
 Reinman, Tzachy

Rekleitis, Evangelos
 Rial, Alfredo
 Rizomiliotis, Panagiotis
 Roman, Rodrigo
 Safa, Nashad Ahmad
 Scafuro, Alessandra
 Schiffner, Stefan
 Shahandashti, Siamak
 Song, Boyeon
 Steel, Graham
 Traore, Jacques
 Troncoso, Carmela
 Tuhin, Ashraful
 Valeontis, Etythios
 Vavitsas, Giorgos
 Vercauteren, Frederik
 Vergnaud, Damien
 Visconti, Ivan
 Vivas, Jose L.
 Vrakas, Nikos
 Wang, Pengwei
 Yoshihama, Sachiko

Table of Contents

RFID and Privacy

A New Framework for RFID Privacy	1
<i>Robert H. Deng, Yingjiu Li, Moti Yung, and Yunlei Zhao</i>	
Readers Behaving Badly: Reader Revocation in PKI-Based RFID Systems	19
<i>Rishab Nithyanand, Gene Tsudik, and Ersin Uzun</i>	
Privacy-Preserving, Taxable Bank Accounts	37
<i>Elli Androulaki, Binh Vo, and Steven Bellovin</i>	
Formal Analysis of Privacy for Vehicular Mix-Zones	55
<i>Morten Dahl, Stéphanie Delaune, and Graham Steel</i>	

Software Security

IntPatch: Automatically Fix Integer-Overflow-to-Buffer-Overflow Vulnerability at Compile-Time	71
<i>Chao Zhang, Tielei Wang, Tao Wei, Yu Chen, and Wei Zou</i>	
A Theory of Runtime Enforcement, with Results	87
<i>Jay Ligatti and Srikar Reddy</i>	
Enforcing Secure Object Initialization in Java	101
<i>Laurent Hubert, Thomas Jensen, Vincent Monfort, and David Pichardie</i>	
Flexible Scheduler-Independent Security	116
<i>Heiko Mantel and Henning Sudbrock</i>	

Cryptographic Protocols

Secure Multiparty Linear Programming Using Fixed-Point Arithmetic	134
<i>Octavian Catrina and Sebastiaan de Hoogh</i>	
A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on Σ -Protocols	151
<i>José Bacelar Almeida, Endre Bangerter, Manuel Barbosa, Stephan Krenn, Ahmad-Reza Sadeghi, and Thomas Schneider</i>	

Short Generic Transformation to Strongly Unforgeable Signature in the Standard Model	168
<i>Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou</i>	

DR@FT: Efficient Remote Attestation Framework for Dynamic Systems	182
<i>Wenjuan Xu, Gail-Joon Ahn, Hongxin Hu, Xinwen Zhang, and Jean-Pierre Seifert</i>	

Traffic Analysis

Website Fingerprinting and Identification Using Ordered Feature Sequences	199
<i>Liming Lu, Ee-Chien Chang, and Mun Choon Chan</i>	

Web Browser History Detection as a Real-World Privacy Threat	215
<i>Artur Janc and Lukasz Olejnik</i>	

On the Secrecy of Spread-Spectrum Flow Watermarks	232
<i>Xiapu Luo, Junjie Zhang, Roberto Perdisci, and Wenke Lee</i>	

Traffic Analysis against Low-Latency Anonymity Networks Using Available Bandwidth Estimation	249
<i>Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis</i>	

End-User Security

A Hierarchical Adaptive Probabilistic Approach for Zero Hour Phish Detection	268
<i>Guang Xiang, Bryan A. Pendleton, Jason Hong, and Carolyn P. Rose</i>	

Kamouflage: Loss-Resistant Password Management	286
<i>Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh</i>	

Formal Analysis

Sequential Protocol Composition in Maude-NPA	303
<i>Santiago Escobar, Catherine Meadows, José Meseguer, and Sonia Santiago</i>	

Verifying Security Property of Peer-to-Peer Systems Using CSP	319
<i>Tien Tuan Anh Dinh and Mark Ryan</i>	

Modeling and Analyzing Security in the Presence of Compromising Adversaries	340
<i>David Basin and Cas Cremers</i>	

On Bounding Problems of Quantitative Information Flow	357
<i>Hirotooshi Yasuoka and Tachio Terauchi</i>	

E-voting and Broadcast

On E-Vote Integrity in the Case of Malicious Voter Computers	373
<i>Sven Heiberg, Helger Lipmaa, and Filip van Laenen</i>	
Election Verifiability in Electronic Voting Protocols	389
<i>Steve Kremer, Mark Ryan, and Ben Smyth</i>	
Pretty Good Democracy for More Expressive Voting Schemes	405
<i>James Heather, Peter Y.A. Ryan, and Vanessa Teague</i>	
Efficient Multi-dimensional Key Management in Broadcast Services	424
<i>Marina Blanton and Keith B. Frikken</i>	

Authentication, Access Control, Authorization and Attestation

Caught in the Maze of Security Standards	441
<i>Jan Meier and Dieter Gollmann</i>	
User-Role Reachability Analysis of Evolving Administrative Role Based Access Control	455
<i>Mikhail I. Gofman, Ruiqi Luo, and Ping Yang</i>	
An Authorization Framework Resilient to Policy Evaluation Failures . . .	472
<i>Jason Crampton and Michael Huth</i>	
Optimistic Fair Exchange with Multiple Arbiters	488
<i>Alptekin Küpçü and Anna Lysyanskaya</i>	

Anonymity and Unlinkability

Speaker Recognition in Encrypted Voice Streams	508
<i>Michael Backes, Goran Doychev, Markus Dürmuth, and Boris Köpf</i>	
Evaluating Adversarial Partitions	524
<i>Andreas Pashalidis and Stefan Schiffner</i>	
Providing Mobile Users' Anonymity in Hybrid Networks	540
<i>Claudio A. Ardagna, Sushil Jajodia, Pierangela Samarati, and Angelos Stavrou</i>	
Complexity of Anonymity for Security Protocols	558
<i>Ferucio Laurențiu Tiplea, Loredana Vamanu, and Cosmin Vârlan</i>	

Network Security and Economics

<i>k</i> -Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks	573
<i>Lingyu Wang, Sushil Jajodia, Anoop Singhal, and Steven Noel</i>	
Are Security Experts Useful? Bayesian Nash Equilibria for Network Security Games with Limited Information	588
<i>Benjamin Johnson, Jens Grossklags, Nicolas Christin, and John Chuang</i>	
RatFish: A File Sharing Protocol Provably Secure against Rational Users	607
<i>Michael Backes, Oana Ciobotaru, and Anton Krohmer</i>	
A Service Dependency Model for Cost-Sensitive Intrusion Response	626
<i>Nizar Kheir, Nora Cuppens-Boulahia, Frédéric Cuppens, and Hervé Debar</i>	

Secure Update, DOS and Intrusion Detection

Secure Code Update for Embedded Devices via Proofs of Secure Erasure	643
<i>Daniele Perito and Gene Tsudik</i>	
D(e i)aling with VoIP: Robust Prevention of DIAL Attacks	663
<i>Alexandros Kapravelos, Iasonas Polakis, Elias Athanasopoulos, Sotiris Ioannidis, and Evangelos P. Markatos</i>	
Low-Cost Client Puzzles Based on Modular Exponentiation	679
<i>Ghassan O. Karame and Srdjan Čapkun</i>	
Expressive, Efficient and Obfuscation Resilient Behavior Based IDS	698
<i>Arnur G. Tokhtabayev, Victor A. Skormin, and Andrey M. Dolgikh</i>	
Author Index	717