Lecture Notes in Computer Science 6345

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

Springer

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

springer.com

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 cooperation.

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

Fan, Junfeng
Fernandez-Gago, Carmen
Fitzgerald, William
Gagne, Marin
Galindo, David
Garcia, Flavio
Garcia-Alfaro, Joaquin
Geneiatakis, Dimitris
Gierlichs, Benedikt
Gouglidis, 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, Eytyhios
Vavitsas, Giorgos
Vercauteren, Frederik
Vergnaud, Damien
Visconti, Ivan
Vivas, Jose L.
Vrakas, Nikos
Wang, Pengwei
Yoshihama, Sachiko

Table of Contents

RFID and Privacy

Software Security

Cryptographic Protocols

Traffic Analysis

End-User Security

Formal Analysis

E-voting and Broadcast

Authentication, Access Control, Authorization and Attestation

Anonymity and Unlinkability

Network Security and Economics

Secure Update, DOS and Intrustion Detection