Lecture Notes in Computer Science 8134

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Jason Crampton Sushil Jajodia
Keith Mayes (Eds.)

Computer Security – ESORICS 2013

18th European Symposium
on Research in Computer Security
Egham, UK, September 9-13, 2013
Proceedings

Springer

Volume Editors

Jason Crampton
Royal Holloway, University of London
Information Security Group
Egham Hill, Egham, TW20 0EX, UK
E-mail: jason.crampton@rhul.ac.uk

Sushil Jajodia
George Mason University
Center for Secure Information Systems
4400 University Drive, Fairfax, VA 22030-4422, USA
E-mail: jajodia@gmu.edu

Keith Mayes
Royal Holloway, University of London
Information Security Group
Egham Hill, Egham, TW20 0EX, UK
E-mail: keith.mayes@rhul.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-40202-9 e-ISBN 978-3-642-40203-6
DOI 10.1007/978-3-642-40203-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013944563

CR Subject Classification (1998): K.6.5, E.3, D.4.6, K.4.4, C.2.0, J.1, H.2.7

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

This volume contains the papers selected for presentation at the 18th European Symposium on Research in Computer Security (ESORICS 2013), held during September 9–13, 2013, in Egham, UK.

In response to the symposium's call for papers, 242 papers were submitted to the conference from 38 countries. These papers were evaluated on the basis of their significance, novelty, technical quality, as well as on their practical impact and/or their level of advancement of the field's foundations.

The Program Committee's work was carried out electronically, yielding intensive discussions over a period of a few weeks. Of the papers submitted, 43 were selected for presentation at the conference (resulting in an acceptance rate of 18%). We note that many top-quality submissions were not selected for presentation because of the high technical level of the overall submissions, and we are certain that many of these submissions will, nevertheless, be published at other competitive forums in the future.

An event like ESORICS 2013 depends on the volunteering efforts of a host of individuals and the support of numerous institutes. There is a long list of people who volunteered their time and energy to put together and organize the conference, and who deserve special thanks. Thanks to all the members of the Program Committee and the external reviewers for all their hard work in evaluating the papers. We are also very grateful to all the people whose work ensured a smooth organization process: the ESORICS Steering Committee, and its Chair Pierangela Samarati in particular, for their support; Giovanni Livraga, for taking care of publicity; Sheila Cobourne, for maintaining the website; and the Local Organizing Committee, for helping with organization and taking care of local arrangements. We would also like to express our appreciation to everyone who organized the workshops (CATACRYPT, Cryptoforma, DPM, EUROPKI, QASA, SETOP, STM, Trustworthy Clouds) co-located with ESORICS. A number of organizations also deserve special thanks, including Royal Holloway University of London for acting as host, and the ESORICS sponsors: CESG, Transport for London, ISG Smart Card Centre, Crisp Telecom Limited, and NESSoS.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the symposium's attendees. We hope you find the proceedings of ESORICS 2013 stimulating and a source of inspiration for your future research and education programs.

September 2013

Jason Crampton
Sushil Jajodia
Keith Mayes

Organization

General Chair

Keith Mayes	Royal Holloway, University of London, UK

Program Chairs

Jason Crampton	Royal Holloway, University of London, UK
Sushil Jajodia	George Mason University, USA

ESORICS Steering Committee

Michael Backes	Saarland University, Germany
Joachim Biskup	University of Dortmund, Germany
Frédéric Cuppens	Télécom Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Yves Deswarte	LAAS, France
Dieter Gollmann	TU Hamburg-Harburg, Germany
Sokratis Katsikas	University of Piraeus, Greece
Miroslaw Kutylowski	Wroclaw University of Technology, Poland
Javier Lopez	University of Malaga, Spain
Jean-Jacques Quisquater	UCL Crypto Group, Belgium
Peter Ryan	University of Luxembourg, Luxembourg
Pierangela Samarati (Chair)	Università degli Studi di Milano, Italy
Einar Snekkenes	Gjøvik University College, Norway
Michael Waidner	TU Darmstadt, Germany

Publicity Chair

Giovanni Livraga	Università degli Studi di Milano, Italy

Local Organizing Committee

Geraint Price	Royal Holloway, University of London, UK
Gerhard Hancke	Royal Holloway, University of London, UK
Kostas Markantonakis	Royal Holloway, University of London, UK
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Sheila Cobourne	Royal Holloway, University of London, UK

Emma Mosley	Royal Holloway, University of London, UK
Jenny Lee	Royal Holloway, University of London, UK

Program Committee

Gail-Joon Ahn	Arizona State University, USA
Massimiliano Albanese	George Mason University, USA
Claudio Agostino Ardagna	Università degli Studi di Milano, Italy
Alessandro Armando	University of Genova, Italy
Michael Backes	Saarland University and Max Planck Institute for Software Systems, Germany
David Basin	ETH Zurich, Switzerland
Kevin Bauer	MIT Lincoln Laboratory, USA
Lujo Bauer	Carnegie Mellon University, USA
Konstantin Beznosov	UBC, Canada
Marina Blanton	University of Notre Dame, USA
Carlo Blundo	Università di Salerno, Italy
Kevin Butler	University of Oregon, USA
Srdjan Capkun	ETH Zurich, Switzerland
Liqun Chen	Hewlett-Packard Laboratories, UK
Sherman S.M. Chow	Chinese University of Hong Kong, SAR China
Marco Cova	University of Birmingham, UK
Jason Crampton	Royal Holloway, University of London, UK
Frédéric Cuppens	TELECOM Bretagne, France
Sabrina De Capitani Di Vimercati	Università degli Studi di Milano, Italy
Roberto Di Pietro	Università di Roma Tre, Italy
Claudia Diaz	K.U. Leuven, Belgium
Josep Domingo-Ferrer	Rovira i Virgili University, Spain
Wenliang Du	Syracuse University, USA
Riccardo Focardi	Università Ca' Foscari di Venezia, Italy
Simon Foley	University College Cork, Ireland
Sara Foresti	Università degli Studi di Milano, Italy
Cedric Fournet	Microsoft, UK
Keith Frikken	Miami University, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Gerhard Hancke	Royal Holloway, University of London, UK
Amir Herzberg	Bar Ilan University, Israel
Michael Huth	Imperial College London, UK
Sushil Jajodia	George Mason University, USA
Aaron Johnson	Naval Research Laboratory, USA
Jonathan Katz	University of Maryland, USA
Stefan Katzenbeisser	TU Darmstadt, Germany
Engin Kirda	Northeastern University, USA

Markulf Kohlweiss	Microsoft Research Cambridge, UK
Steve Kremer	INRIA Nancy - Grand Est, France
Miroslaw Kutylowski	Wroclaw University of Technology, Poland
Adam J. Lee	University of Pittsburgh, USA
Wenke Lee	Georgia Institute of Technology, USA
Yingjiu Li	Singapore Management University, Singapore
Benoit Libert	Technicolor, France
Javier Lopez	University of Malaga, Spain
Wenjing Lou	Virginia Polytechnic Institute and State University, USA
Pratyusa K Manadhata	HP Labs, USA
Luigi Mancini	Università di Roma La Sapienza, Italy
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Gregory Neven	IBM Zurich Research Laboratory, Switzerland
Stefano Paraboschi	Università di Bergamo, Italy
Kenneth Paterson	Royal Holloway, University of London, UK
Dusko Pavlovic	Royal Holloway, University of London, UK
Günther Pernul	Universität Regensburg, Germany
Frank Piessens	Katholieke Universiteit Leuven, Belgium
Michalis Polychronakis	Columbia University, USA
Alexander Pretschner	Technische Universität München, Germany
Kui Ren	State University of New York at Buffalo, USA
Mark Ryan	University of Birmingham, UK
P.Y.A. Ryan	University of Luxembourg, Luxembourg
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Ahmad-Reza Sadeghi	TU Darmstadt, Germany
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Radu Sion	Stony Brook University, USA
Nigel Smart	University of Bristol, UK
Einar Snekkenes	Gjvik University College, Norway
Vipin Swarup	The MITRE Corporation, USA
Roberto Tamassia	Brown University, USA
Carmela Troncoso	IBBT-K.U.Leuven, ESAT/COSIC, Belgium
Yevgeniy Vahlis	University of Toronto, Canada
Jaideep Vaidya	Rutgers University, USA
Vijay Varadharajan	Macquarie University, Australia
Venkat Venkatakrishnan	University of Illinois at Chicago, USA
Luca Viganò	University of Verona, Italy
Michael Waidner	Fraunhofer SIT, Germany
Bogdan Warinschi	University of Bristol, USA
Ting Yu	North Carolina State University, USA
Moti Yung	Google and Columbia University, USA

Additional Reviewers

Ahmadi, Ahmad
Alfardan, Nadhem
Aliasgari, Mehrdad
Alimomeni, Mohsen
Androulaki, Elli
Arriaga, Afonso
Asharov, Gilad
Balsa, Ero
Banescu, Sebastian
Basu, Anirban
Batten, Ian
Baum, Carsten
Beato, Filipe
Ben Hamouda, Fabrice
Bertolissi, Clara
Bkakria, Anis
Blaskiewicz, Przemyslaw
Boyd, Colin
Bozzato, Claudio
Broser, Christian
Brzuska, Christina
Cachin, Christian
Calvi, Alberto
Calzavara, Stefano
Carbone, Roberto
Catalano, Dario
Chandran, Nishanth
Chen, Jiageng
Chen, Ling
Chen, Si
Chen, Xihui
Cheval, Vincent
Choo, Euijin
Collberg, Christian
Cremers, Cas
Cuppens-Boulahia, Nora
Datta, Anupam
De Benedictis, Alessandra
De Caro, Angelo
De Groef, Willem
De Ryck, Philippe
Del Tedesco, Filippo
Delaune, Stéphanie
Devriese, Dominique
Du, Changlai
Durgin, Nancy
Epasto, Alessandro
Farnan, Nicholas
Farràs, Oriol
Ferdman, Mike
Fernandez-Gago, Carmen
Fitzgerald, William Michael
Frank, Mario
Fromm, Alexander
Fuchs, Andreas
Fuchs, Ludwig
Futa, Yuichi
Gajek, Sebastian
Galbraith, Steven
Galindo, David
Garrison, William
Gasti, Paolo
Gelernter, Nethanel
George, Wesley
Ghiglieri, Marco
Gilad, Yossi
Giustolisi, Rosario
Gjomemo, Rigel
Goberman, Michael
Grewal, Gurchetan S.
Hadi Ahmadi, Ashish Kisti
Hajian, Sara
Hanzlik, Lucjan
Hedin, Daniel
Herfert, Michael
Herrmann, Michael
Heuser, Stephan
Hoens, T. Ryan
Holzer, Andreas
Hosek, Petr
Idrees, Sabir
Jansen, Rob
Jhawar, Mahavir
Jia, Limin
Joaquim, Rui
Jonker, Hugo

Jorgensen, Zachery
Joye, Marc
Kalabis, Lukas
Kamara, Seny
Keppler, David
Khader, Dalia
Klaedtke, Felix
Kluczniak, Kamil
Komanduri, Saranga
Konidala, Divyan
Kordy, Barbara
Kostiainen, Kari
Krzywiecki, Lukasz
Kubiak, Przemysław
Kumari, Prachi
Kywe, Su Mon
Künnemann, Robert
Lancrenon, Jean
Li, Jin
Li, Yan
Liu, Jia
Livraga, Giovanni
Lochbihler, Andreas
Loftus, Jake
Lombardi, Flavio
Lovat, Enrico
Ma, Di
Magazinius, Jonas
Majcher, Krzysztof
Malacaria, Pasquale
Malisa, Luka
Manulis, Mark
Marinovic, Srdjan
Mathur, Suhas
Maurice, Clementine
Mazurek, Michelle
Meadows, Catherine
Meier, Stefan
Min, Byungho
Mitrou, Lilian
Moataz, Tarik
Molinaro, Cristian
Mood, Benjamin
Moyano, Francisco
Muehlberg, Jan Tobias
Mutti, Simone
Mylonas, Alexis
Netter, Michael
Nikiforakis, Nick
Nojoimian, Mehrdad
Nuñez, David
Oligeri, Gabriele
Omote, Kazumasa
Orlandi, Claudio
Oswald, Elisabeth
Oya, Simon
Palazzi, Bernardo
Pang, Jun
Paterson, Maura
Paul, Giura
Peacock, Thea
Peeters, Roel
Peroli, Michele
Peters, Thomas
Petit, Jonathan
Phillips, Joshua
Pieczul, Olgierd
Pinto, Alexandre
Poettering, Bertram
Pujol, Marta
Qin, Zhan
Radomirovic, Sasa
Rafnsson, Willard
Ranganathan, Aanjhan
Ranise, Silvio
Reisser, Andreas
Rial, Alfredo
Riesner, Moritz
Rijmen, Vincent
Riva, Ben
Roman, Rodrigo
Saracino, Andrea
Sayaf, Rula
Scerri, Guillaume
Schneider, Thomas
Schuldt, Jacob
Schulz, Steffen
Schunter, Matthias
Sepehrdad, Pouyan
Sgandurra, Daniele

Shafiq, Basit
Shakarian, Paulo
Shen, Entong
Shi, Jie
Shirazi, Fatemeh
Shulman, Haya
Simo, Hervais
Smans, Jan
Smith, Geoffrey
Soria Comas, Jordi
Soriente, Claudio
Soupionis, Yannis
Squarcina, Marco
Stebila, Douglas
Stefanov, Emil
Stopczynski, Martin
Struminski, Tomasz
Sun, Wenhai
Syverson, Paul
Tews, Erik
Theoharidou, Marianthi
Torabi Dashti, Mohammad
Toz, Deniz
Tsoumas, Bill
Tuerpe, Sven
Tupakula, Uday
Van Acker, Steven
Verde, Nino Vincenzo
Villani, Antonio
Virvilis, Nick
Vitali, Domenico
Wachsmann, Christian
Wang, Bing
Wang, Lusha
Watson, Gaven J.
Weber, Michael
Wei, Wei
Wüchner, Tobias
Yan, Qiben
Yautsiukhin, Artsiom
Yu, Jiangshan
Zagorski, Filip
Zanella-Béguelin, Santiago
Zhang, Bingsheng
Zhang, Liang Feng
Zhang, Ning
Zhang, Tao
Zhang, Xifan
Zhang, Yihua
Zhou, Lan
Zugenmaier, Alf

Table of Contents

Cryptography and Computation

Measurement and Evaluation

Applications of Cryptography

Code Analysis

Network Security

Formal Models and Methods

Protocol Analysis

Privacy Enhancing Models and Technologies

E-voting and Privacy

Malware Detection

Access Control

Attacks

Language-Based Protection