Lecture Notes in Computer Science 5789

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

Michael Backes Peng Ning (Eds.)

Computer Security – ESORICS 2009

14th European Symposium on Research in Computer Security
Saint-Malo, France, September 21-23, 2009
Proceedings

Springer

Volume Editors

Michael Backes
Saarland University
Computer Science Department and MPI-SWS
Building E1.1, Campus, 66123 Saarbrücken, Germany
E-mail: backes@mpi-sws.mpg.de

Peng Ning
North Carolina State University
Department of Computer Science
3320 Engineering Building II, Raleigh, NC 27695-8206, USA
E-mail: pning@ncsu.edu

Library of Congress Control Number: 2009934436

CR Subject Classification (1998): E.3, K.6.5, K.4.4, C.2, D.4.6, H.2.7

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-04443-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-04443-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12755578 06/3180 5 4 3 2 1 0

Foreword from the General Chairs

We warmly welcome everyone to the proceedings of ESORICS 2009, the 14th European Symposium on Research in Computer Security. This year, ESORICS was held in a beautiful walled port city in Brittany in north-western France during September 21–23. We hope that the serenity of Saint-Malo and the high quality of ESORICS 2009 papers facilitated a stimulating exchange of ideas among many members of our international research community.

This year, we were pleased to be holding RAID 2009 in conjunction with ESORICS 2009. The conference was followed on September 24-25 by three workshops: DPM 2009 was the 4th International Workshop on Data Privacy Management, SETOP 2009 was the Second International Workshop on Autonomous and Spontaneous Security organized/sponsored by the TELECOM Institute, and STM 2009 was the 5th workshop on Security and Trust Management. Thus, we had a high-quality week of research and debate on computer security.

ESORICS 2009 was made possible only through the hard work of many people. Michael Backes and Peng Ning assembled an outstanding Technical Program Committee that reviewed submitted papers and selected an exciting and high-quality technical program. We were most fortunate to have Michael and Peng as Program Chairs to keep ESORICS on a path of academic excellence and practical relevance; we express our sincere thanks to both of them. A debt of thanks is due to our Program Committee members and external reviewers for helping to assemble such a strong technical program.

We thank particularly Gilbert Martineau, our Sponsor Chair for his rigorous and unfailing work. We would like also to thank our PHD student, Julien Thomas, who helped us in creating and managing the website. Without the help of the Publicity Chair, ESORICS 2009 would not have had such a success; so, many thanks to Sara Foresti.

We are also very grateful to our sponsors: DCSSI, INRIA, Rennes Métropole, Région Bretagne, Fondation Métivier, Saint-Malo, Alcatel-Lucent Bell Labs France, EADS, Orange, TELECOM Institute and CG35. Their generosity helped keep the costs of ESORICS 2009 moderate.

We thank everyone, merci, for attending the conference and being a part of this very important event.

September 2009

Frédéric Cuppens
Nora Cuppens-Boulahia

Foreword from the Program Co-chairs

It is our great pleasure to welcome you to the proceedings of the 14th European Symposium on Research in Computer Security (ESORICS 2009), which was held in Saint Malo, France, September 21–23, 2009. ESORICS has become the European research event in computer security. The symposium started in 1990 and has been organized on alternate years in different European countries. From 2002 it has taken place yearly. It attracts an international audience from both the academic and industrial communities. In response to the call for papers, 220 papers were submitted to the symposium. These papers were evaluated on the basis of their significance, novelty, and technical quality. The majority of these papers went through two rounds of reviews, evaluated by at least three members of the Program Committee. The Program Committee meeting was held electronically, holding intensive discussion over a period of one month since the completion of the first round of reviews. Finally, 42 papers were selected for presentation at the symposium, giving an acceptance rate of 19%.

There is a long list of people who volunteered their time and energy to put together the symposium and who deserve acknowledgment. Our thanks to the General Chairs, Frédéric Cuppens and Nora Cuppens-Boulahia, for their valuable support in the organization of the event. Also, to Sara Foresti for the publicity of ESORICS 2009, to Gilbert Martineau for industry sponsorship, to Julien A. Thomas for preparation and maintenance of the symposium website, and to Stefan Lorenz for setting up and maintaining the submission server. Special thanks to the members of the Program Committee and external reviewers for all their hard work during the review and the selection process. Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope that you will find the proceedings stimulating and a source of inspiration for future research.

September 2009

Michael Backes
Peng Ning

Organization

General Co-chairs

Frédéric Cuppens	TELECOM Bretagne, France
Nora Cuppens-Boulahia	TELECOM Bretagne, France

Program Co-chairs

Michael Backes	Saarland University and MPI-SWS, Germany
Peng Ning	North Carolina State University, USA

Publicity Chair

Sara Foresti	University of Milan, Italy

Sponsor Chair

Gilbert Martineau	TELECOM Bretagne, France

Web Chair

Julien A. Thomas	TELECOM Bretagne, France

Program Committee

Mike Atallah	Purdue University, USA
Michael Backes	Saarland University and MPI-SWS, Germany (Co-chair)
David Basin	ETH Zurich, Switzerland
Nikita Borisov	University of Illinois at Urbana-Champaign, USA
Srdjan Capkun	ETH Zurich, Switzerland
Veronique Cortier	LORIA, France
Marc Dacier	EURECOM, France
Anupam Datta	Carnegie Mellon University, USA
Herve Debar	France TELECOM R&D, France
Roger Dingledine	The Tor Project, USA
Wenliang Du	Syracuse University, USA
Cédric Fournet	Microsoft Research Cambridge, UK
Virgil Gligor	Carnegie Mellon University, USA

Guofei Gu	Texas A&M University, USA
Carl A. Gunter	University of Illinois at Urbana-Champaign, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Sushil Jajodia	George Mason University, USA
Xuxian Jiang	North Carolina State University, USA
Peeter Laud	University of Tartu, Estonia
Wenke Lee	Georgia Institute of Technology, USA
Donggang Liu	University of Texas at Arlington, USA
Michael Locasto	George Mason University, USA
Wenjing Lou	Worcester Polytechnic Institute, USA
Matteo Maffei	Saarland University, Germany
Heiko Mantel	University of Darmstadt, Germany
Catherine Meadows	Naval Research Laboratory, USA
John Mitchell	Stanford University, USA
David Molnar	University of California at Berkeley, USA
Peng Ning	North Carolina State University, USA (Co-chair)
Alina Oprea	RSA, USA
Radia Perlman	Sun Microsystems, USA
Adrian Perrig	Carnegie Mellon University, USA
Douglas Reeves	North Carolina State University, USA
Kui Ren	Illinois Institute of Technology, USA
Mark Ryan	University of Birmingham, UK
Pierangela Samarati	Università degli Studi di Milano, Italy
Vitaly Shmatikov	University of Texas at Austin, USA
Wade Trappe	Rutgers University, USA
Patrick Traynor	Georgia Institute of Technology, USA
Dominique Unruh	Saarland University, Germany
Luca Vigano	University of Verona, Italy
Dan S. Wallach	Rice University, USA
Andreas Wespi	IBM Research, Switzerland
Ting Yu	North Carolina State University, USA
Yanyong Zhang	Rutgers University, USA
Xiaolan Zhang	IBM Research, USA

External Reviewers

Pedro Adao	Samuel Burri	Jason Franklin
Myrto Arapinis	Ning Cao	Deepak Garg
Karthikeyan Bhargavan	Sabrina De Capitani di Vimercati	Richard Gay
Bruno Blanchet	Pu Duan	Mike Grace
Johannes Borgstroem	Stelios Dritsas	Rachel Greenstadt
Achim Brucker	Mario Frank	Nataliya Guts
Ahto Buldas		Amir Houmansadr

Sonia Jahid
Karthick Jayaraman
Guenter Karjoth
Emilia Kasper
Dilsun Kaynar
Felix Klaedtke
Panos Kotzanikolaou
Dimitris Lekkas
Ming Li
Alexander Lux
Weiqin Ma
Yannis Mallios
Isabella Mastroeni
Amir Houmansadr
Sebastian Moedersheim
Tamara Rezk
Arnab Roy
Silvio Ranise
Patrick Schaller
Ravinder Shankesi
Dieter Schuster
Ben Smyth
Alessandro Sorniotti
Barbara Sprick
Henning Sudbrock
Michael Tschantz
Marianthi Theoharidou
Bill Tsoumas
Guan Wang
Zhi Wang
Zhenyu Yang
Yiqun Yin
Shucheng Yu
Charles C. Zhang
Dazhi Zhang
Lei Zhang
Zutao Zhu

Sponsoring Institutions

Alcatel-Lucent Bell Labs France
CG35
DCSSI
EADS
Fondation Métivier
INRIA
Orange
Rennes Métropole
Région Bretagne
TELECOM Institute
Ville de Saint de Malo

Table of Contents

Network Security I

Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones 1
Thorsten Holz, Markus Engelberth, and Felix Freiling

User-Centric Handling of Identity Agent Compromise 19
Daisuke Mashima, Mustaque Ahamad, and Swagath Kannan

The Coremelt Attack 37
Ahren Studer and Adrian Perrig

Information Flow

Type-Based Analysis of PIN Processing APIs 53
Matteo Centenaro, Riccardo Focardi, Flaminia L. Luccio, and Graham Steel

Declassification with Explicit Reference Points 69
Alexander Lux and Heiko Mantel

Tracking Information Flow in Dynamic Tree Structures 86
Alejandro Russo, Andrei Sabelfeld, and Andrey Chudnov

Network Security II

Lightweight Opportunistic Tunneling (LOT) 104
Yossi Gilad and Amir Herzberg

Hide and Seek in Time — Robust Covert Timing Channels 120
Yali Liu, Dipak Ghosal, Frederik Armknecht, Ahmad-Reza Sadeghi, Steffen Schulz, and Stefan Katzenbeisser

Authentic Time-Stamps for Archival Storage 136
Alina Oprea and Kevin D. Bowers

Language Based Security

Towards a Theory of Accountability and Audit 152
Radha Jagadeesan, Alan Jeffrey, Corin Pitcher, and James Riely

Reliable Evidence: Auditability by Typing 168
Nataliya Guts, Cédric Fournet, and Francesco Zappa Nardelli

PCAL: Language Support for Proof-Carrying Authorization Systems ... 184
Avik Chaudhuri and Deepak Garg

Network Security III

ReFormat: Automatic Reverse Engineering of Encrypted Messages 200
Zhi Wang, Xuxian Jiang, Weidong Cui, Xinyuan Wang, and Mike Grace

Protocol Normalization Using Attribute Grammars 216
Drew Davidson, Randy Smith, Nic Doyle, and Somesh Jha

Automatically Generating Models for Botnet Detection 232
Peter Wurzinger, Leyla Bilge, Thorsten Holz, Jan Goebel, Christopher Kruegel, and Engin Kirda

Access Control

Dynamic Enforcement of Abstract Separation of Duty Constraints 250
David Basin, Samuel J. Burri, and Günter Karjoth

Usable Access Control in Collaborative Environments: Authorization Based on People-Tagging 268
Qihua Wang, Hongxia Jin, and Ninghui Li

Requirements and Protocols for Inference-Proof Interactions in Information Systems 285
Joachim Biskup, Christian Gogolin, Jens Seiler, and Torben Weibert

Privacy - I

A Privacy Preservation Model for Facebook-Style Social Network Systems 303
Philip W.L. Fong, Mohd Anwar, and Zhen Zhao

New Privacy Results on Synchronized RFID Authentication Protocols against Tag Tracing 321
Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini

Secure Pseudonymous Channels 337
Sebastian Mödersheim and Luca Viganò

Distributed Systems Security

Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing 355
Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou

Content Delivery Networks: Protection or Threat? 371
Sipat Triukose, Zakaria Al-Qudah, and Michael Rabinovich

Model-Checking DoS Amplification for VoIP Session Initiation 390
Ravinder Shankesi, Musab AlTurki, Ralf Sasse, Carl A. Gunter, and José Meseguer

Privacy - II

The Wisdom of Crowds: Attacks and Optimal Constructions 406
George Danezis, Claudia Diaz, Emilia Käsper, and Carmela Troncoso

Secure Evaluation of Private Linear Branching Programs with Medical Applications 424
Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Ahmad-Reza Sadeghi, and Thomas Schneider

Keep a Few: Outsourcing Data While Maintaining Confidentiality 440
Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati

Security Primitives

Data Structures with Unpredictable Timing 456
Darrell Bethea and Michael K. Reiter

WORM-SEAL: Trustworthy Data Retention and Verification for Regulatory Compliance 472
Tiancheng Li, Xiaonan Ma, and Ninghui Li

Corruption-Localizing Hashing 489
Giovanni Di Crescenzo, Shaoquan Jiang, and Reihaneh Safavi-Naini

Web Security

Isolating JavaScript with Filters, Rewriting, and Wrappers 505
Sergio Maffeis, John C. Mitchell, and Ankur Taly

An Effective Method for Combating Malicious Scripts Clickbots 523
Yanlin Peng, Linfeng Zhang, J. Morris Chang, and Yong Guan

Client-Side Detection of XSS Worms by Monitoring Payload Propagation 539
Fangqi Sun, Liang Xu, and Zhendong Su

Cryptography

Formal Indistinguishability Extended to the Random Oracle Model 555
Cristian Ene, Yassine Lakhnech, and Van Chan Ngo

Computationally Sound Analysis of a Probabilistic Contract Signing Protocol 571
Mihhail Aizatulin, Henning Schnoor, and Thomas Wilke

Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption 587
Rakesh Bobba, Himanshu Khurana, and Manoj Prabhakaran

Protocols

A Generic Security API for Symmetric Key Management on Cryptographic Devices 605
Véronique Cortier and Graham Steel

ID-Based Secure Distance Bounding and Localization 621
Nils Ole Tippenhauer and Srdjan Čapkun

Secure Ownership and Ownership Transfer in RFID Systems 637
Ton van Deursen, Sjouke Mauw, Saša Radomirović, and Pim Vullers

Systems Security and Forensics

Cumulative Attestation Kernels for Embedded Systems 655
Michael LeMay and Carl A. Gunter

Super-Efficient Aggregating History-Independent Persistent Authenticated Dictionaries 671
Scott A. Crosby and Dan S. Wallach

Set Covering Problems in Role-Based Access Control 689
Liang Chen and Jason Crampton

Author Index 705