Lecture Notes in Computer Science 6879

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

Vijay Atluri Claudia Diaz (Eds.)

Computer Security – ESORICS 2011

16th European Symposium
on Research in Computer Security
Leuven, Belgium, September 12-14, 2011
Proceedings

Springer

Volume Editors

Vijay Atluri
Rutgers University
MSIS Department and CIMIC
1 Washington Park
Newark, NJ 07102, USA
E-mail: atluri@rutgers.edu

Claudia Diaz
K.U. Leuven ESAT/COSIC
Kasteelpark Arenberg 10
3001 Leuven-Heverlee, Belgium
E-mail: claudia.diaz@esat.kuleuven.be

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-23821-5 e-ISBN 978-3-642-23822-2
DOI 10.1007/978-3-642-23822-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011935429

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.
The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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

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

ESORICS 2011 was the 16th edition of the event. It was held in Leuven, Belgium, during September 12–14, 2011. The conference received 155 submissions. The papers went through a careful review process in which each paper received at least three independent reviews. The papers were then discussed by the Program Committee to arrive to the final decision. The Program Committee selected 36 papers for the final program, resulting in an acceptance rate of 23%. 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 Ross Anderson, from the University of Cambridge.

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 Bart Preneel, the General Chair of this symposium, for his continuous support. Our appreciation goes to Claudio Ardagna for acting as Publicity Chair; and to Pela Noe, Saartje Verheyen, Sebastiaan Indesteege, Roel Peeters, and the rest of the COSIC team for their help with the organization of the event. We are also grateful to Google, Technicolor, and BCRYPT for sponsoring ESORICS 2011.

Finally, we would like to thank the submitters, authors, presenters, and participants who, all together, made ESORICS 2011 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 toward an on-line world with adequate security.

June 2011

Vijay Atluri
Claudia Diaz

Organization

General Chair

Bart Preneel	K.U. Leuven, Belgium

Program Committee Chairs

Vijay Atluri	Rutgers University, USA
Claudia Diaz	K.U. Leuven, Belgium

Publicity Chair

Claudio Ardagna	Università degli Studi di Milano, Italy

Program Committee Members

Mikhail Atallah	Purdue University, USA
Michael Backes	Saarland University and MPI-SWS, Germany
Feng Bao	Institute for Infocomm Research, Singapore
Lujo Bauer	Carnegie Mellon University, USA
Carlo Blundo	Università di Salerno, Italy
Jan Camenisch	IBM Research - Zurich, Switzerland
Srdjan Capkun	ETH Zurich, Switzerland
Véronique Cortier	LORIA-CNRS, France
Jason Crampton	Royal Holloway, University of London, UK
Frédéric Cuppens	IT TELECOM Bretagne,France
George Danezis	Microsoft Research, UK
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Roger Dingledine	The Tor Project, USA
Orr Dunkelman	Weizmann Institute, Israel
Simon Foley	University College Cork, Ireland
Dieter Gollmann	Hamburg University of Technology, Germany
Thorsten Holz	Ruhr University Bochum, Germany
Sushil Jajodia	George Mason University, USA
Stefan Katzenbeisser	T.U. Darmstadt, Germany
Angelos Keromytis	Columbia University, USA
Aggelos Kiayias	University of Athens, Greece
Michiharu Kudo	IBM Research - Tokyo, Japan
Klaus Kursawe	University of Nijmegen, The Netherlands
Adam Lee	University of Pittsburgh, USA

Ronald Leenes	Tilburg University / TILT, The Netherlands
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
David Molnar	Microsoft Research, USA
Steven Murdoch	University of Cambridge, UK
Gregory Neven	IBM Research - Zurich, Switzerland
Radia Perlman	Intel Corporation, USA
Indrakshi Ray	Colorado State University, USA
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Rei Safavi-Naini	University of Calgary, Calgary
Pierangela Samarati	Università degli Studi di Milano, Italy
R. Sekar	Stony Brook University, USA
Basit Shafiq	Rutgers University, USA
Vitaly Shmatikov	University of Texas Austin, USA
Einar Snekkenes	Gjovik University College, Norway
Paul Syverson	Naval Research Laboratory, USA
Patrick Traynor	Georgia Institute of Technology, USA
Carmela Troncoso	K.U. Leuven, Belgium
Jaideep Vaidya	Rutgers University, USA
Will Winsborough	University of Texas at San Antonio, USA

External Reviewers

Zahra Aghazadeh
Hadi Ahmadi
Mohsen Alimomeni
Sami Alsouri
Todd Andel
Elena Andreeva
George Argyros
Md. Shamim Ashik
Elias Athanasopoulos
Ero Balsa
Manuel Barbosa
Lejla Batina
Meriam Ben Ghorbel
Joseph Bonneau
Mike Brennan
Sven Bugiel
Joan Calvet
Sambuddho Chakravarty
Omar-Salim Choudary
Omar Chowdhury
Cheng-Kang Chu
Cas Cremers
Nora Cuppens-Boulahia
Paolo D'Arco
Jun Dai
Angelo De Caro
Emiliano De Cristofaro
Elke De Mulder
Mario Di Raimondo
Maria Dubovitskaya
Nicholas Farnan
Carmen Fernández-Gago
Sara Foresti
Aurelien Francillon
Martin Franz
Keith Frikken
Martin Gagne
Joaquin Garcia-Alfaro
Deepak Garg
Dimitris Geneiatakis
Johannes Hoffmann
Yuan Hong
Ralf Hund
Vincenzo Iovino
Rob Jansen
Kangkook Jee
Ravi Jhawar
Aaron Johnson
Ghassan Karame
Charlie Kaufman
Vasileios P. Kemerlis
Johannes Kinder
Marc Kuehrer
Hoi Le
Fengjun Li
Joseph Liu
Giovanni Livraga
Mohammad Hossein Manshaei
Claudio Marforio
Damon Mccoy
Nicky Mouha
Francisco Moyano
Sascha Müller
Pablo Najera
Kris Narayan

Ana Nieto
David Nuñez
Femi Olumofin
Vasilis Pappas
Andreas Pashalidis
Cristina Perez
Ray Perlner
Michalis Polychronakis
Murillo Pontual
Christina Popper
Georgios Portokalidis
David Ramos
Aanjhan Ranganathan
Indrajit Ray
Joel Reardon
David Rebollo-Monedero
Ruben Rios
Rodrigo Roman
Ahmad-Reza Sadeghi
Nashad Safa
Thomas Schneider
Steffen Schulz
Reza Shokri
Ben Smyth
Angelos Stavrou
Kun Sun
Xiaoyan Sun
Gelareh Taban
Mehdi Talbi
Naoki Tanaka
Nils Tippenhauer
Mathieu Turuani
Sebastian Uellenbeck
Jeffrey Vaughan
Jose Luis Vivas
Christian Wachsmann
Jun Wang
Gaven Watson
Marcel Winandy
Yongdong Wu
Ji Xiang
Xi Xiong
Yanjiang Yang
Eugen Zalinescu
Qiang Zeng
Bin Zhao
Wanying Zhao

Table of Contents

Wireless Security

Secure Localization Using *Dynamic Verifiers* 1
Nashad A. Safa, Saikat Sarkar, Reihaneh Safavi-Naini, and Majid Ghaderi

WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection 21
Diogo Mónica and Carlos Ribeiro

Investigation of Signal and Message Manipulations on the Wireless Channel 40
Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun

Web Security I

Protecting Private Web Content from Embedded Scripts 60
Yuchen Zhou and David Evans

Preventing Web Application Injections with Complementary Character Coding 80
Raymond Mui and Phyllis Frankl

Automatic and Precise Client-Side Protection against CSRF Attacks . . . 100
Philippe De Ryck, Lieven Desmet, Wouter Joosen, and Frank Piessens

Web Security II

Timing Is Everything: The Importance of History Detection 117
Gunnar Kreitz

Reclaiming the Blogosphere, TalkBack: A Secure LinkBack Protocol for Weblogs 133
Elie Bursztein, Baptiste Gourdin, and John C. Mitchell

A Systematic Analysis of XSS Sanitization in Web Application Frameworks 150
Joel Weinberger, Prateek Saxena, Devdatta Akhawe, Matthew Finifter, Richard Shin, and Dawn Song

Forensics, Biometrics and Software Protection

Who Wrote This Code? Identifying the Authors of Program Binaries ... 172
Nathan Rosenblum, Xiaojin Zhu, and Barton P. Miller

Secure and Efficient Protocols for Iris and Fingerprint Identification 190
Marina Blanton and Paolo Gasti

Linear Obfuscation to Combat Symbolic Execution 210
Zhi Wang, Jiang Ming, Chunfu Jia, and Debin Gao

DriverGuard: A Fine-Grained Protection on I/O Flows 227
Yueqiang Cheng, Xuhua Ding, and Robert H. Deng

Access Control

Time-Storage Trade-Offs for Cryptographically-Enforced Access Control 245
Jason Crampton

Socially Constructed Trust for Distributed Authorization 262
Steve Barker and Valerio Genovese

Fully Secure Multi-authority Ciphertext-Policy Attribute-Based Encryption without Random Oracles 278
Zhen Liu, Zhenfu Cao, Qiong Huang, Duncan S. Wong, and Tsz Hon Yuen

Cryptography and Protocol Analysis

How to Aggregate the CL Signature Scheme 298
Dominique Schröder

Key Exchange in IPsec Revisited: Formal Analysis of IKEv1 and IKEv2 315
Cas Cremers

Adapting Helios for Provable Ballot Privacy 335
David Bernhard, Véronique Cortier, Olivier Pereira, Ben Smyth, and Bogdan Warinschi

Information Flow, Side Channels, and Vulnerability Analysis

Remote Timing Attacks Are Still Practical 355
Billy Bob Brumley and Nicola Tuveri

Multi-run Security 372
Arnar Birgisson and Andrei Sabelfeld

Automated Information Flow Analysis of Virtualized Infrastructures 392
Sören Bleikertz, Thomas Groß, Matthias Schunter, and Konrad Eriksson

Scalable Analysis of Attack Scenarios 416
Massimiliano Albanese, Sushil Jajodia, Andrea Pugliese, and V.S. Subrahmanian

Usability, Ttrust, and Economics of Security and Privacy

Usability of Display-Equipped RFID Tags for Security Purposes 434
Alfred Kobsa, Rishab Nithyanand, Gene Tsudik, and Ersin Uzun

Forcing Johnny to Login Safely: Long-Term User Study of Forcing and Training Login Mechanisms 452
Amir Herzberg and Ronen Margulies

Towards a Mechanism for Incentivating Privacy 472
Piero A. Bonatti, Marco Faella, Clemente Galdi, and Luigi Sauro

Investigating the OpenPGP Web of Trust 489
Alexander Ulrich, Ralph Holz, Peter Hauck, and Georg Carle

Privacy I

A Practical Complexity-Theoretic Analysis of Mix Systems 508
Dang Vinh Pham, Joss Wright, and Dogan Kesdogan

A Light-Weight Solution to Preservation of Access Pattern Privacy in Un-trusted Clouds 528
Ka Yang, Jinsheng Zhang, Wensheng Zhang, and Daji Qiao

Optimizing Mixing in Pervasive Networks: A Graph-Theoretic Perspective 548
Murtuza Jadliwala, Igor Bilogrevic, and Jean-Pierre Hubaux

Privacy II

A New RFID Privacy Model 568
Jens Hermans, Andreas Pashalidis, Frederik Vercauteren, and Bart Preneel

Quantitative Information Flow, with a View 588
Michele Boreale, Francesca Pampaloni, and Michela Paolini

To Release Or Not to Release: Evaluating Information Leaks in Aggregate Human-Genome Data 607
Xiaoyong Zhou, Bo Peng, Yong Fuga Li, Yangyi Chen, Haixu Tang, and XiaoFeng Wang

Privacy III

Don't Reveal My Intension: Protecting User Privacy Using Declarative Preferences during Distributed Query Processing 628
Nicholas L. Farnan, Adam J. Lee, Panos K. Chrysanthis, and Ting Yu

Supporting Concurrency in Private Data Outsourcing 648
Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Gerardo Pelosi, and Pierangela Samarati

Privacy-Preserving DNS: Analysis of Broadcast, Range Queries and Mix-Based Protection Methods 665
Hannes Federrath, Karl-Peter Fuchs, Dominik Herrmann, and Christopher Piosecny

Author Index 685