

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zürich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Günther Pernul · Peter Y A Ryan  
Edgar Weippl (Eds.)

# Computer Security – ESORICS 2015

20th European Symposium on Research in Computer Security  
Vienna, Austria, September 21–25, 2015  
Proceedings, Part I

*Editors*

Günther Pernul  
University of Regensburg  
Regensburg  
Germany

Edgar Weippl  
SBA Research  
Wien  
Austria

Peter Y A Ryan  
University of Luxembourg  
Luxembourg  
Luxembourg

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-24173-9              ISBN 978-3-319-24174-6 (eBook)  
DOI 10.1007/978-3-319-24174-6

Library of Congress Control Number: 2015948157

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London  
© Springer International Publishing Switzerland 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media  
([www.springer.com](http://www.springer.com))

# Foreword

It is our great pleasure to welcome you to the 20<sup>th</sup> European Symposium on Research in Computer Security (ESORICS 2015).

This year's symposium continues its tradition of establishing a European forum for bringing together researchers in the area of computer security, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

The call for papers attracted 293 submissions – a record in the ESORICS series – from 41 countries. The papers went through a careful review process and 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. Each paper received at least three independent reviews, followed by extensive discussion. We finally selected 59 papers for the final program, resulting in an acceptance rate of 20 %.

The program was completed with keynote speeches by Sushil Jajodia, George Mason University Fairfax, USA and Richard Clayton, University of Cambridge, UK.

Putting together ESORICS 2015 was a team effort. We first thank the authors for providing the content of the program. We are grateful to the Program Committee, who worked very hard in reviewing papers (more than 880 reviews were written) and providing feedback for authors. 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: the ESORICS Steering Committee, and its chair Pierangela Samarati in particular, for their support; Giovanni Livraga, for taking care of publicity; Javier Lopez, as workshop chair, and all workshop co-chairs, who organized workshops co-located with ESORICS; and Yvonne Poul for the local organization and the social events.

Finally, we would like to thank our sponsors, HUAWEI, for the financial support and SBA Research, for hosting and organizing ESORICS 2015.

A different country hosts the conference every year. ESORICS 2015 took place in Vienna, Austria at the Vienna University of Technology. We are very happy to have hosted the 20<sup>th</sup> edition of the symposium in Vienna and we tried to put together a special social program for you, giving you the opportunity to share ideas with other researchers and practitioners from institutions around the world and see all the beautiful sights of Vienna.

We hope that you found this program interesting and thought-provoking and that you enjoyed ESORICS 2015 and Vienna.

July 2015

Günther Pernul  
Peter Y A Ryan  
Edgar Weippl



Dieter Gollmann	TU Hamburg-Harburg, Germany
Dimitris Gritzalis	AUEB, Greece
Joshua Guttman	MTIRE Corp and Worcester Polytechnic, USA
Feng Hao	Newcastle University, UK
Amir Herzberg	Bar-Ilan University, Israel
Xinyi Huang	Fujian Normal University, China
Michael Huth	Imperial College, UK
Sotiris Ioannidis	FORTH, Crete
Sushil Jajodia	George Mason University, USA
Markus Jakobsson	Qualcomm, USA
Sokratis K. Katsikas	University of Piraeus, Greece
Stefan Katzenbeisser	TU Darmstadt, Germany
Florian Kerschbaum	SAP, Germany
Steve Kremer	INRIA Nancy and LORIA, France
Adam J. Lee	University of Pittsburgh, USA
Wenke Lee	Georgia Institute of Technology, USA
Yingjiu Li	Singapore Management University, Singapore
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Wenjing Lou	Virginia Polytechnic Institute and State University, USA
Haibing Lu	Santa Clara University, USA
Antonio Maña	Univeristy of Malaga, Spain
Roy Maxion	Carnegie Mellon University, USA
Catherine Meadows	Naval Research Laboratory, USA
Carroll Morgan	University of New South Wales, Australia
John C. Mitchell	Stanford University, USA
Martin Mulazzani	SBA Research, Austria
David Naccache	ENS, France
Rolf Oppliger	eSecurity Technologies, Switzerland
Stefano Paraboschi	Università degli Studi di Bergamo, Italy
Olivier Pereira	UCL Crypto Group, Belgium
Günther Pernul	University of Regensburg, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater	UCL, Belgium
Kui Ren	University at Buffalo, State University of New York, USA
Mark Ryan	University of Birmingham, UK
Ahmad-Reza Sadeghi	TU Darmstadt, Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Nitesh Saxena	University of Alabama at Birmingham, USA
Andreas Schaad	SAP, Germany
Steve Schneider	University of Surrey, UK
Jörg Schwenk	Ruhr University Bochum, Germany
Basit Shafiq	Lahore University of Management Sciences, Pakistan
Dimitris E. Simos	SBA Research, Austria

Einar Snekkenes	Gjøvik University College, Norway
Philip Stark	University of California, Berkeley, USA
Vanessa Teague	University of Melbourne, Australia
Jaideep Vaidya	Rutgers University, USA
Paulo Verissimo	University of Luxembourg, Luxembourg
Luca Viganò	King's College London, UK
Michael Waidner	TU Darmstadt, Germany
Cong Wang	City University of Hong Kong, China
Lingyu Wang	University of Concordia, Canada
Ting Yu	North Carolina State University, USA
Meng Yu	Virginia Commonwealth University, USA
Moti Yung	Google, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Sencun Zhu	Pennsylvania State University, USA



# Contents – Part I

## Networks and Web Security

- Towards Security of Internet Naming Infrastructure . . . . . 3  
*Haya Shulman and Michael Waidner*
- Waiting for CSP – Securing Legacy Web Applications with JSAgents . . . . . 23  
*Mario Heiderich, Marcus Niemietz, and Jörg Schwenk*
- Analyzing the BrowserID SSO System with Primary Identity Providers  
Using an Expressive Model of the Web . . . . . 43  
*Daniel Fett, Ralf Küsters, and Guido Schmitz*

## System Security

- A Practical Approach for Adaptive Data Structure Layout Randomization . . . 69  
*Ping Chen, Jun Xu, Zhiqiang Lin, Dongyan Xu, Bing Mao, and Peng Liu*
- Trustworthy Prevention of Code Injection in Linux on Embedded Devices . . . 90  
*Hind Chfouka, Hamed Nemati, Roberto Guanciale, Mads Dam,  
and Patrik Ekdahl*
- Practical Memory Deduplication Attacks in Sandboxed Javascript . . . . . 108  
*Daniel Gruss, David Bidner, and Stefan Mangard*

## Cryptography

- Computational Soundness for Interactive Primitives . . . . . 125  
*Michael Backes, Esfandiar Mohammadi, and Tim Ruffing*
- Verifiably Encrypted Signatures: Security Revisited and a New  
Construction . . . . . 146  
*Christian Hanser, Max Rabkin, and Dominique Schröder*
- Interleaving Cryptanalytic Time-Memory Trade-Offs on Non-uniform  
Distributions . . . . . 165  
*Gildas Avoine, Xavier Carpent, and Cédric Lauradoux*
- Efficient Message Authentication Codes with Combinatorial Group Testing . . . 185  
*Kazuhiko Minematsu*

Symmetric-Key Based Proofs of Retrievability Supporting Public Verification . . . . .	203
<i>Chaowen Guan, Kui Ren, Fangguo Zhang, Florian Kerschbaum, and Jia Yu</i>	
DTLS-HIMMO: Achieving DTLS Certificate Security with Symmetric Key Overhead . . . . .	224
<i>Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, and Jose Luis Torre-Arce</i>	
Short Accountable Ring Signatures Based on DDH. . . . .	243
<i>Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit</i>	
Updatable Hash Proof System and Its Applications . . . . .	266
<i>Rupeng Yang, Qiuliang Xu, Yongbin Zhou, Rui Zhang, Chengyu Hu, and Zuoxia Yu</i>	
Server-Aided Revocable Identity-Based Encryption . . . . .	286
<i>Baodong Qin, Robert H. Deng, Yingjiu Li, and Shengli Liu</i>	
Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings. . . . .	305
<i>Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak</i>	
Making <b>Any</b> Identity-Based Encryption Accountable, Efficiently . . . . .	326
<i>Aggelos Kiayias and Qiang Tang</i>	
Practical Threshold Password-Authenticated Secret Sharing Protocol . . . . .	347
<i>Xun Yi, Feng Hao, Liqun Chen, and Joseph K. Liu</i>	
On Security of Content-Based Video Stream Authentication . . . . .	366
<i>Swee-Won Lo, Zhuo Wei, Robert H. Deng, and Xuhua Ding</i>	
Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification . . . . .	384
<i>Marina Blanton and Siddharth Saraph</i>	
Practical Invalid Curve Attacks on TLS-ECDH. . . . .	407
<i>Tibor Jager, Jörg Schwenk, and Juraj Somorovsky</i>	
<b>Crypto Applications and Attacks</b>	
Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-Proof? . . .	429
<i>Alessandro Barenghi, Alessandro Di Federico, Gerardo Pelosi, and Stefano Sanfilippo</i>	

Transforming Out Timing Leaks, More or Less . . . . . 447  
*Heiko Mantel and Artem Starostin*

Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE  
 Implementations in 3G/4G USIM Cards. . . . . 468  
*Junrong Liu, Yu Yu, François-Xavier Standaert, Zheng Guo, Dawu Gu,  
 Wei Sun, Yijie Ge, and Xinjun Xie*

**Risk Analysis**

Should Cyber-Insurance Providers Invest in Software Security? . . . . . 483  
*Aron Laszka and Jens Grossklags*

Lightweight and Flexible Trust Assessment Modules for the Internet  
 of Things. . . . . 503  
*Jan Tobias Mühlberg, Job Noorman, and Frank Piessens*

Confidence Analysis for Nuclear Arms Control: SMT Abstractions  
 of Bayesian Belief Networks . . . . . 521  
*Paul Beaumont, Neil Evans, Michael Huth, and Tom Plant*

**Author Index** . . . . . 541

## Contents – Part II

### Privacy

<i>FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting . . . . .</i>	3
<i>Christof Ferreira Torres, Hugo Jonker, and Sjouke Mauw</i>	
Mind-Reading: Privacy Attacks Exploiting Cross-App KeyEvent Injections. . . . .	20
<i>Wenrui Diao, Xiangyu Liu, Zhe Zhou, Kehuan Zhang, and Zhou Li</i>	
Enabling Privacy-Assured Similarity Retrieval over Millions of Encrypted Records . . . . .	40
<i>Xingliang Yuan, Helei Cui, Xinyu Wang, and Cong Wang</i>	
Privacy-Preserving Link Prediction in Decentralized Online Social Networks . . . . .	61
<i>Yao Zheng, Bing Wang, Wenjing Lou, and Y. Thomas Hou</i>	
Privacy-Preserving Observation in Public Spaces. . . . .	81
<i>Florian Kerschbaum and Hoon Wei Lim</i>	
Privacy-Preserving Context-Aware Recommender Systems: Analysis and New Solutions . . . . .	101
<i>Qiang Tang and Jun Wang</i>	

### Cloud Security

Rich Queries on Encrypted Data: Beyond Exact Matches. . . . .	123
<i>Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel Rosu, and Michael Steiner</i>	
Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data . . . . .	146
<i>Yanjiang Yang, Joseph K. Liu, Kaitai Liang, Kim-Kwang Raymond Choo, and Jianying Zhou</i>	
Batch Verifiable Computation of Polynomials on Outsourced Data . . . . .	167
<i>Liang Feng Zhang and Reihaneh Safavi-Naini</i>	
CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud . . . . .	186
<i>Qian Wang, Shengshan Hu, Kui Ren, Meiqi He, Minxin Du, and Zhibo Wang</i>	

**Protocols and Attribute-Based Encryption**

Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment. . . . . 209  
*Omar Almousa, Sebastian Mödersheim, Paolo Modesti, and Luca Viganò*

Checking Trace Equivalence: How to Get Rid of Nonces? . . . . . 230  
*Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune*

Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key . . . . . 252  
*Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Xiaofeng Chen*

Accountable Authority Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud . . . . . 270  
*Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei*

**Code Analysis and Side-Channels**

DexHunter: Toward Extracting Hidden Code from Packed Android Applications. . . . . 293  
*Yueqian Zhang, Xiapu Luo, and Haoyang Yin*

Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software . . . . . 312  
*Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena*

vBox: Proactively Establishing Secure Channels Between Wireless Devices Without Prior Knowledge. . . . . 332  
*Wei Wang, Jingqiang Lin, Zhan Wang, Ze Wang, and Luning Xia*

**Detection and Monitoring**

Accurate Specification for Robust Detection of Malicious Behavior in Mobile Environments. . . . . 355  
*Sufatrio, Tong-Wei Chua, Darell J.J. Tan, and Vrizlynn L.L. Thing*

A Bytecode Interpreter for Secure Program Execution in Untrusted Main Memory . . . . . 376  
*Maximilian Seitzer, Michael Gruhn, and Tilo Müller*

Learning from Others: User Anomaly Detection Using Anomalous Samples from Other Users . . . . . 396  
*Youngja Park, Ian M. Molloy, Suresh N. Chari, Zenglin Xu, Chris Gates, and Ninghi Li*

**Authentication**

Towards Attack-Resistant Peer-Assisted Indoor Localization. . . . . 417  
*Jingyu Hua, Shaoyong Du, and Sheng Zhong*

Leveraging Real-Life Facts to Make Random Passwords More Memorable. . . . . 438  
*Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright,  
 and Shannon Scielzo*

The Emperor’s New Password Creation Policies:: An Evaluation  
 of Leading Web Services and the Effect of Role in Resisting Against  
 Online Guessing . . . . . 456  
*Ding Wang and Ping Wang*

**Policies**

A Theory of Gray Security Policies. . . . . 481  
*Donald Ray and Jay Ligatti*

Factorization of Behavioral Integrity . . . . . 500  
*Ximeng Li, Flemming Nielson, and Hanne Riis Nielson*

Checking Interaction-Based Declassification Policies for Android  
 Using Symbolic Execution . . . . . 520  
*Kristopher Micinski, Jonathan Fetter-Degges, Jinseong Jeon,  
 Jeffrey S. Foster, and Michael R. Clarkson*

**Applied Security**

Enhancing Java Runtime Environment for Smart Cards Against  
 Runtime Attacks . . . . . 541  
*Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes*

Making Bitcoin Exchanges Transparent . . . . . 561  
*Christian Decker, James Guthrie, Jochen Seidel, and Roger Wattenhofer*

Web-to-Application Injection Attacks on Android: Characterization  
 and Detection . . . . . 577  
*Behnaz Hassanshahi, Yaoqi Jia, Roland H.C. Yap, Prateek Saxena,  
 and Zhenkai Liang*

All Your Voices are Belong to Us: Stealing Voices to Fool Humans  
 and Machines . . . . . 599  
*Dibya Mukhopadhyay, Maliheh Shirvanian, and Nitesh Saxena*

Balloon: A Forward-Secure Append-Only Persistent Authenticated  
 Data Structure. . . . . 622  
*Tobias Pulls and Roel Peeters*

On the Fly Design and Co-simulation of Responses Against Simultaneous Attacks . . . . .	642
<i>Léa Samarji, Nora Cuppens-Boulahia, Frédéric Cuppens, Serge Papillon, Waël Kanoun, and Samuel Dubus</i>	
<b>Author Index</b> . . . . .	663