Lecture Notes in Computer Science 8713

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

Mirosław Kutyłowski Jaideep Vaidya (Eds.)

Computer Security – ESORICS 2014

19th European Symposium
on Research in Computer Security
Wrocław, Poland, September 7-11, 2014
Proceedings, Part II

Springer

Volume Editors

Mirosław Kutyłowski
Wrocław University of Technology
Wrocław, Poland
E-mail: miroslaw.kutylowski@pwr.edu.pl

Jaideep Vaidya
Rutgers, The State University of New Jersey
Newark, NJ, USA
E-mail: jsvaidya@business.rutgers.edu

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-11211-4 e-ISBN 978-3-319-11212-1
DOI 10.1007/978-3-319-11212-1
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014947642

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

These volumes contain the papers selected for presentation at the 19th European Symposium on Research in Computer Security (ESORICS 2014), held during September 7–11, 2014, in Wrocław, Poland. ESORICS has a two-decade-old tradition of bringing together the international research community in a top-quality event that covers all the areas of computer security, ranging from theory to applications.

In response to the symposium's call for papers, 234 papers were submitted to the conference from 38 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 58 papers for the final program, resulting in an acceptance rate of 24.79%. The authors of accepted papers were requested to revise their papers, based on the comments received. The program was completed with invited talks by Moti Yung from Google Inc. and Columbia University, Stefano Paraboschi from Università di Bergamo, and Shlomi Dolev from Ben Gurion University of the Negev. A special talk on privacy protection was given by Wojciech Wiewiórowski, Inspector General for Personal Data Protection in Poland.

An event like ESORICS 2014 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. We are indebted to Jacek Cichoń, the general chair of this symposium, for his continuous support. 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; Małgorzata Korzeniowska for management of the local arrangements, Kamil Kluczniak for the technical work of putting the proceedings together; and the local Organizing Committee, in particular Przemysław Kobylański, Maciej Gebala, and Wojciech Wodo, for helping with organization and taking care of local arrangements. We would also like to express our appreciation to everyone who organized the workshops (BADGERS, DPM, QASA, SETOP SloT, STM, Smart ConDev S&P, UaESMC) co-located with ESORICS. A number of organizations also deserve special thanks, including Wrocław University of Technology for acting as host, National Cryptology Centre as a partner institution, and the ESORICS sponsors.

Finally, we would like to thank the submitters, authors, presenters, and participants who, all together, made ESORICS 2014 a great success. We hope that

the papers in these volumes 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 and privacy.

September 2014

Mirosław Kutyłowski
Jaideep Vaidya

Organization

Program Committee

Masayuki Abe	NTT Secure Platform Laboratories, Japan
Gail-Joon Ahn	Arizona State University, USA
Mikhail Atallah	Purdue University, USA
Vijay Atluri	Rutgers University, USA
Michael Backes	Saarland University, Germany
Kun Bai	IBM T.J. Watson Research Center, USA
Giampaolo Bella	Universitá di Catania, Italy
Marina Blanton	University of Notre Dame, USA
Kevin Butler	University of Oregon, USA
Zhenfu Cao	Shanghai-Jiao Tong University, PR China
Srdjan Capkun	ETH Zurich, Switzerland
Liqun Chen	Hewlett-Packard Laboratories, UK
Xiaofeng Chen	Xidian University, PR China
Sherman S.M. Chow	Chinese University of Hong Kong, SAR China
Veronique Cortier	CNRS, LORIA, France
Marco Cova	University of Birmingham, UK
Laszlo Csirmaz	Central European University, Budapest, Hungary
Frederic Cuppens	TELECOM Bretagne, France
Nora Cuppens-Boulahia	TELECOM Bretagne, France
Reza Curtmola	New Jersey Institute of Technology, USA
Ozgur Dagdelen	Technische Universität Darmstadt, Germany
Sabrina De Capitani Di Vimercati	Università degli Studi di Milano, Italy
Roberto Di Pietro	Università di Roma Tre, Italy
Claudia Diaz	KU Leuven, Belgium
Josep Domingo-Ferrer	Università Rovira i Virgili, Catalonia
Wenliang Du	Syracuse University, USA
Simon Foley	University College Cork, Ireland
Philip W.L. Fong	University of Calgary, Canada
Sara Foresti	Università degli Studi di Milano, Italy
Keith Frikken	Miami University, Ohio, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Ehud Gudes	Ben-Gurion University, Israel
Thorsten Holz	Ruhr University Bochum, Germany

Yuan Hong	University at Albany, SUNY, USA
Xinyi Huang	Fujian Normal University, PR China
Sushil Jajodia	George Mason University, USA
Sokratis Katsikas	University of Piraeus, Greece
Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
Florian Kerschbaum	SAP, Germany
Kwangjo Kim	KAIST, Korea
Marek Klonowski	Wrocław University of Technology, Poland
Wenke Lee	Georgia Institute of Technology, USA
Adam J. Lee	University of Pittsburgh, USA
Helger Lipmaa	University of Tartu, Estonia
Peng Liu	The Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Haibing Lu	Santa Clara University, USA
Emil Lupu	Imperial College, UK
Mark Manulis	University of Surrey, UK
Krystian Matusiewicz	Intel Technology Poland
Christoph Meinel	Hasso-Plattner-Institut, Germany
Refik Molva	EURECOM, France
David Naccache	Ecole Normale Suprieure, France
Stefano Paraboschi	Università di Bergamo, Italy
Gunther Pernul	Universität Regensburg, Germany
Indrakshi Ray	Colorado State University, USA
Christian Rechberger	Technical University of Denmark
Kui Ren	University of Buffalo, SUNY, USA
Ahmad-Reza Sadeghi	Technische Universität Darmstadt, Germany
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Andreas Schaad	SAP, Germany
Basit Shafiq	Lahore University of Management Sciences, Pakistan
Radu Sion	Stony Brook University, USA
Shamik Sural	IIT, Kharagpur, India
Willy Susilo	University of Wollongong, Australia
Krzysztof Szczypiorski	Warsaw University of Technology, Poland
Mahesh Tripunitara	The University of Waterloo, Canada
Michael Waidner	Fraunhofer SIT, Germany
Lingyu Wang	Concordia University, Canada
Yang Xiang	Deakin University, Australia
Xun Yi	Victoria University, Australia
Ting Yu	Qatar Computing Research Institute, Qatar
Meng Yu	Virginia Commonwealth University, USA
Rui Zhang	Chinese Academy of Sciences, PR China
Jianying Zhou	Institute for Infocomm Research, Singapore

Table of Contents – Part II

Public-Key Revocation and Tracing Schemes with Subset Difference Methods Revisited 1
Kwangsu Lee, Woo Kwon Koo, Dong Hoon Lee, and Jong Hwan Park

NORX: Parallel and Scalable AEAD 19
Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves

Even More Practical Secure Logging: Tree-Based Seekable Sequential Key Generators 37
Giorgia Azzurra Marson and Bertram Poettering

Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability 55
Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and Xiaodong Lin

PPDCP-ABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption 73
Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Au

Practical Direct Chosen Ciphertext Secure Key-Policy Attribute-Based Encryption with Public Ciphertext Test 91
Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, and Yunya Zhou

Privacy-Preserving Auditing for Attribute-Based Credentials 109
Jan Camenisch, Anja Lehmann, Gregory Neven, and Alfredo Rial

What's the Gist? Privacy-Preserving Aggregation of User Profiles 128
Igor Bilogrevic, Julien Freudiger, Emiliano De Cristofaro, and Ersin Uzun

Challenging Differential Privacy: The Case of Non-interactive Mechanisms 146
Raghavendran Balu, Teddy Furon, and Sébastien Gambs

Optimality and Complexity of Inference-Poof Data Filtering and CQE 165
Joachim Biskup, Piero A. Bonatti, Clemente Galdi, and Luigi Sauro

New Insight to Preserve Online Survey Accuracy and Privacy in Big Data Era 182
Joseph K. Liu, Man Ho Au, Xinyi Huang, Willy Susilo, Jianying Zhou, and Yong Yu

Software Countermeasures for Control Flow Integrity of Smart Card C Codes 200
Jean-François Lalande, Karine Heydemann, and Pascal Berthomé

LeakWatch: Estimating Information Leakage from Java Programs 219
Tom Chothia, Yusuke Kawamoto, and Chris Novakovic

SigPath: A Memory Graph Based Approach for Program Data Introspection and Modification 237
David Urbina, Yufei Gu, Juan Caballero, and Zhiqiang Lin

ID-Based Two-Server Password-Authenticated Key Exchange 257
Xun Yi, Feng Hao, and Elisa Bertino

Modelling Time for Authenticated Key Exchange Protocols 277
Jörg Schwenk

Zero-Knowledge Password Policy Checks and Verifier-Based PAKE 295
Franziskus Kiefer and Mark Manulis

Bitcoin Transaction Malleability and MtGox 313
Christian Decker and Roger Wattenhofer

Election Verifiability for Helios under Weaker Trust Assumptions 327
Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachène

CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin 345
Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate

LESS Is More: Host-Agent Based Simulator for Large-Scale Evaluation of Security Systems 365
John Sonchack and Adam J. Aviv

Detecting Insider Information Theft Using Features from File Access Logs 383
Christopher Gates, Ninghui Li, Zenglin Xu, Suresh N. Chari, Ian Molloy, and Youngja Park

SRID: State Relation Based Intrusion Detection for False Data Injection Attacks in SCADA 401
Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, and Guofei Gu

Click Fraud Detection on the Advertiser Side 419
Haitao Xu, Daiping Liu, Aaron Koehl, Haining Wang, and Angelos Stavrou

Botyacc: Unified P2P Botnet Detection Using Behavioural Analysis and Graph Analysis 439
Shishir Nagaraja

Feature-Distributed Malware Attack: Risk and Defence 457
Byungho Min and Vijay Varadharajan

RootkitDet: Practical End-to-End Defense against Kernel Rootkits in a Cloud Environment 475
Lingchen Zhang, Sachin Shetty, Peng Liu, and Jiwu Jing

Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks 494
Lingyu Wang, Mengyuan Zhang, Sushil Jajodia, Anoop Singhal, and Massimiliano Albanese

Author Index 513

Table of Contents – Part I

Detecting Malicious Domains via Graph Inference 1
Pratyusa K. Manadhata, Sandeep Yadav, Prasad Rao, and William Horne

Empirically Measuring WHOIS Misuse 19
Nektarios Leontiadis and Nicolas Christin

EncDNS: A Lightweight Privacy-Preserving Name Resolution Service . . . 37
Dominik Herrmann, Karl-Peter Fuchs, Jens Lindemann, and Hannes Federrath

Ubic: Bridging the Gap between Digital Cryptography and the Physical World 56
Mark Simkin, Dominique Schröder, Andreas Bulling, and Mario Fritz

Updaticator: Updating Billions of Devices by an Efficient, Scalable and Secure Software Update Distribution over Untrusted Cache-enabled Networks 76
Moreno Ambrosin, Christoph Busold, Mauro Conti, Ahmad-Reza Sadeghi, and Matthias Schunter

Local Password Validation Using Self-Organizing Maps 94
Diogo Mónica and Carlos Ribeiro

Verifiable Delegation of Computations with Storage-Verification Trade-off 112
Liang Feng Zhang and Reihaneh Safavi-Naini

Identity-Based Encryption with Post-Challenge Auxiliary Inputs for Secure Cloud Applications and Sensor Networks 130
Tsz Hon Yuen, Ye Zhang, Siu Ming Yiu, and Joseph K. Liu

Verifiable Computation over Large Database with Incremental Updates 148
Xiaofeng Chen, Jin Li, Jian Weng, Jianfeng Ma, and Wenjing Lou

DroidMiner: Automated Mining and Characterization of Fine-grained Malicious Behaviors in Android Applications 163
Chao Yang, Zhaoyan Xu, Guofei Gu, Vinod Yegneswaran, and Phillip Porras

Detecting Targeted Smartphone Malware with Behavior-Triggering Stochastic Models 183
Guillermo Suarez-Tangil, Mauro Conti, Juan E. Tapiador, and Pedro Peris-Lopez

TrustDump: Reliable Memory Acquisition on Smartphones 202
He Sun, Kun Sun, Yuewu Wang, Jiwu Jing, and Sushil Jajodia

A Framework to Secure Peripherals at Runtime 219
Fengwei Zhang, Haining Wang, Kevin Leach, and Angelos Stavrou

StealthGuard: Proofs of Retrievability with Hidden Watchdogs 239
Monir Azraoui, Kaoutar Elkhiyaoui, Refik Molva, and Melek Önen

An Efficient Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme for Public Clouds Data Sharing 257
Kaitai Liang, Joseph K. Liu, Duncan S. Wong, and Willy Susilo

Verifiable Computation on Outsourced Encrypted Data 273
Junzuo Lai, Robert H. Deng, Hweehwa Pang, and Jian Weng

Verifiable Computation with Reduced Informational Costs and Computational Costs 292
Gang Xu, George T. Amariucai, and Yong Guan

Detangling Resource Management Functions from the TCB in Privacy-Preserving Virtualization 310
Min Li, Zili Zha, Wanyu Zang, Meng Yu, Peng Liu, and Kun Bai

Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage 326
Yujue Wang, Qianhong Wu, Duncan S. Wong, Bo Qin, Sherman S.M. Chow, Zhen Liu, and Xiao Tan

Quantitative Workflow Resiliency 344
John C. Mace, Charles Morisset, and Aad van Moorsel

Who Is Touching My Cloud 362
Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi

A Fast Single Server Private Information Retrieval Protocol with Low Communication Cost 380
Changyu Dong and Liqun Chen

Privacy-Preserving Complex Query Evaluation over Semantically Secure Encrypted Data 400
Bharath Kumar Samanthula, Wei Jiang, and Elisa Bertino

Authorized Keyword Search on Encrypted Data 419
Jie Shi, Junzuo Lai, Yingjiu Li, Robert H. Deng, and Jian Weng

Double-Authentication-Preventing Signatures 436
Bertram Poettering and Douglas Stebila

Statistical Properties of Pseudo Random Sequences and Experiments with PHP and Debian OpenSSL 454
Yongge Wang and Tony Nicol

Efficient Hidden Vector Encryption with Constant-Size Ciphertext 472
Tran Viet Xuan Phuong, Guomin Yang, and Willy Susilo

Enabling Short Fragments for Uncoordinated Spread Spectrum Communication 488
Naveed Ahmed, Christina Pöpper, and Srdjan Capkun

Fingerprinting Far Proximity from Radio Emissions 508
Tao Wang, Yao Liu, and Jay Ligatti

A Cross-Layer Key Establishment Scheme in Wireless Mesh Networks 526
Yuexin Zhang, Yang Xiang, Xinyi Huang, and Li Xu

Author Index 543