

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, Zurich, 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>

Ioannis Askoxylakis · Sotiris Ioannidis
Sokratis Katsikas · Catherine Meadows (Eds.)

Computer Security – ESORICS 2016

21st European Symposium on Research in Computer Security
Heraklion, Greece, September 26–30, 2016
Proceedings, Part I

Editors

Ioannis Askoxylakis
Institute of Computer Science
Foundation for Research and
Technology - Hellas
Heraklion
Greece

Sotiris Ioannidis
Institute of Computer Science
Foundation for Research and
Technology - Hellas
Heraklion
Greece

Sokratis Katsikas
Norwegian University of Science and
Technology
Gjøvik
Norway

Catherine Meadows
Naval Research Laboratory
Washington, DC
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-45743-7 ISBN 978-3-319-45744-4 (eBook)
DOI 10.1007/978-3-319-45744-4

Library of Congress Control Number: 2016949626

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 2016

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

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

This volume contains papers selected for presentation and publication at the 21st European Symposium on Research in Computer Security, ESORICS, held September 26–30, in Heraklion, Greece.

Out of 285 submissions from 40 countries, the conference accepted 60 papers, resulting in an acceptance rate of 21 %. These papers cover a wide range of topics in security and privacy, including data protection, systems security, network security, access control, authentication, and security in such emerging areas as cloud computing, cyber-physical systems, and the Internet of Things. The papers were reviewed and then discussed online by a 105-member Program Committee, along with 313 external reviewers.

ESORICS 2016 would not have been possible without the contributions of the many volunteers who devoted their time and energy to make this happen. We would like to thank the Program Committee and the external reviewers for their hard work in evaluating the papers. We would also like to thank the ESORICS Steering Committee and its Chair Pierangela Samarati; the Publicity Chairs, Manolis Stamatogiannakis and Youki Kadobayashi; the Local Arrangement Committee, Nikolaos Petroulakis, Andreas Miaoudakis, and Panos Chatziadam, for arranging the beautiful location in Crete; the workshop chair, Javier Lopez, and all workshop co-chairs, who organized workshops co-located with ESORICS. We also give thanks to the many institutions for their support of ESORICS: the Horizon 2020 projects SHARCS and Virtuwind, the Hellenic Authority for Communication Security and Privacy (ADAE), the European Agency for Network and Information Security (ENISA), Huawei Technologies Co., Bournemouth University, and the CIPSEC project.

Finally, we would like to give our thanks to the authors who submitted their papers to ESORICS. They, more than anyone else, are what makes this conference possible.

Welcome to ESORICS 2016!

July 2016

Ioannis Askoxylakis
Sotiris Ioannidis
Sokratis Katsikas
Catherine Meadows

Organization

General Chairs

Ioannis Askoxylakis

Hellenic Authority for Communication Security
and Privacy (ADAE) & FORTH, Greece

Sotiris Ioannidis

FORTH, Greece

Program Chairs

Sokratis K. Katsikas

Norwegian University of Science and Technology,
Norway

Catherine Meadows

Naval Research Laboratory, USA

Workshops Chair

Javier Lopez

University of Malaga, Spain

Program Committee

Gail-Joon Ahn

Arizona State University, USA

Magnus Almgren

Chalmers University of Technology, Sweden

Manos Antonakakis

Georgia Institute of Technology, USA

Alessandro Armando

DIBRIS - University of Genoa, Italy

Michael Backes

Saarland University and Max Planck Institute
for Software Systems, Germany

Giampaolo Bella

Università degli studi di Catania, Italy

Carlo Blundo

Università degli Studi di Salerno, Italy

Stefan Brunthaler

SBA Research, Austria

Rainer Böhme

University of Innsbruck, Austria

Christian Cachin

IBM Research - Zurich, Switzerland

Liquan Chen

Hewlett Packard Labs, UK

Tom Chothia

University of Birmingham, UK

Sherman S.M. Chow

Chinese University of Hong Kong, Hong Kong

Cas Cremers

University of Oxford, UK

Frédéric Cuppens

Telecom Bretagne, France

Nora Cuppens-Boulahia

Telecom Bretagne, France

Mads Dam

KTH, Sweden

Sabrina De Capitani
di Vimercati

Università degli Studi di Milano, Italy

Hervé Debar

Télécom SudParis, France

Roberto Di Pietro

Bell Labs, France

Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Pavlos Efraimidis	Democritus University of Thrace, Greece
Hannes Federrath	University of Hamburg, Germany
Bao Feng	Huawei, China
Simone Fischer-Hübner	Karlstad University, Sweden
Riccardo Focardi	Università Ca' Foscari, Italy
Simon Foley	University College Cork, Ireland
Sara Foresti	Università degli Studi di Milano, Italy
Katrin Franke	Norwegian University of Science and Technology, Norway
Felix Freiling	Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Dieter Gollmann	Hamburg University of Technology, Germany
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Joshua Guttman	Worcester Polytechnic Institute & MITRE, USA
Gerhard Hancke	City University of Hong Kong, China
Marit Hansen	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany
Feng Hao	Newcastle University, UK
Xinyi Huang	Fujian Normal University, China
Michael Huth	Imperial College London, UK
Aaron D. Jaggard	U.S. Naval Research Laboratory, USA
Sushil Jajodia	George Mason University, USA
Vasilios Katos	Bournemouth University, UK
Dogan Kesdogan	Universität Regensburg, Germany
Kwangjo Kim	Korea Advanced Institute of Science and Technology-KAIST, South Korea
Steve Kremer	Inria Nancy - Grand Est, France
Ralf Küsters	University of Trier, Germany
Junzuo Lai	Singapore Management University, Singapore
Costas Lambrinouidakis	University of Piraeus, Greece
Peeter Laud	Cybernetica AS, Estonia
Adam J. Lee	University of Pittsburgh, USA
Ninghui Li	Purdue University, USA
Yingjiu Li	Singapore Management University, Singapore
Antonio Lioy	Politecnico di Torino, Italy
Peng Liu	The Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Pratyusa K. Manadhata	Hewlett-Packard Laboratories, USA
Luigi V. Mancini	Università di Roma "La Sapienza", Italy
Heiko Mantel	TU Darmstadt, Germany
Olivier Markowitch	Université Libre de Bruxelles (ULB), Belgium
Fabio Martinelli	IIT-CNR, Italy
Antonio Maña	University of Malaga, Spain
John Mitchell	Stanford University, USA

Aikaterini Mitrokotsa	Chalmers University of Technology, Sweden
Refik Molva	EURECOM, France
Charles Morisset	Newcastle University, UK
Flemming Nielson	Technical University of Denmark, Denmark
Rolf Oppliger	eSECURITY Technologies, Switzerland
Stefano Paraboschi	Università di Bergamo, Italy
Dusko Pavlovic	University of Hawaii, USA
Roberto Perdisci	University of Georgia, USA
Olivier Pereira	Université catholique de Louvain, Belgium
Günther Pernul	Universität Regensburg, Germany
Wolter Pieters	Delft University of Technology, The Netherlands
Michalis Polychronakis	Stony Brook University, USA
Joachim Posegga	University of Passau, Germany
Kui Ren	State University of New York at Buffalo, USA
Mark Ryan	University of Birmingham, UK
Peter Y.A. Ryan	University of Luxembourg, Luxembourg
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Ravi Sandhu	University of Texas at San Antonio, USA
Ralf Sasse	ETH Zürich, Switzerland
Nitesh Saxena	University of Alabama at Birmingham, USA
Andreas Schaad	Huawei European Research Center, Germany
Steve Schneider	University of Surrey, UK
Joerg Schwenk	Ruhr-Universität Bochum, Germany
Basit Shafiq	Lahore University of Management Sciences, Pakistan
Ben Smyth	Huawei, France
Einar Snekkenes	Norwegian University of Science and Technology, Norway
Willy Susilo	University of Wollongong, Australia
Krzysztof Szczypiorski	Warsaw University of Technology, Poland
A Min Tjoa	Vienna University of Technology, Austria
Aggeliki Tsohou	Ionian University, Greece
Jaideep Vaidya	Rutgers University, USA
Vijay Varadharajan	Macquarie University, Australia
Luca Viganò	King's College London, UK
Michael Waidner	Fraunhofer SIT and TU Darmstadt, Germany
Cong Wang	City University of Hong Kong, China
Edgar Weippl	SBA Research, Austria
Christos Xenakis	University of Piraeus, Greece
Meng Yu	University of Texas at San Antonio, USA
Ben Zhao	University of California at Santa Barbara, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Sencun Zhu	The Pennsylvania State University, USA

Additional Reviewers

Ahmed, Tahmina	Dai, Ting	Hitaj, Briland
Akand, Mamun	Davies, Philip	Horst, Matthias
Ali, Mohammed	De Gaspari, Fabio	Hu, Wenhui
Aliberti, Giulio	De Meo, Federico	Huang, Heqing
Aminanto, Muhamad Erza	Dehnel-Wild, Martin	Huang, Qiong
Anagnostopoulos, Marios	Denzel, Michael	Hummer, Matthias
Anand, S. Abhishek	Dimitriadis, Antonios	Iliadis, John
Asghari, Hadi	Djoko, Judicael	Imran-Daud, Malik
Asif, Hafiz	Dreier, Jannik	Iovino, Vincenzo
Axelsson, Stefan	Drogkaris, Prokopios	Iwaya Horn, Leonardo
Bacis, Enrico	Drosatos, George	Jackson, Dennis
Balliu, Musard	Elkhiyaoui, Kaoutar	Jager, Tibor
Bardas, Alexandru G.	Emms, Martin	Jarecki, Stanislaw
Batten, Ian	Engelke, Toralf	Jasser, Stefanie
Baumann, Christoph	Espes, David	Jiang, Hemin
Bayou, Lyes	Fahl, Sascha	Journault, Anthony
Bello, Luciano	Farràs, Oriol	Kamm, Liina
Berrang, Pascal	Fett, Daniel	Kandias, Miltos
Bhatt, Sandeep	Fuchs, Ludwig	Karegar, Farzaneh
Biswas, Bhaskar	Garratt, Luke	Karopoulos, George
Blanco-Justicia, Alberto	Garrison, William	Koshutanski, Hristo
Bruni, Alessandro	Gay, Richard	Koutsiamanis,
Bugiel, Sven	Geneiatakis, Dimitris	Remous Aris
Calzavara, Stefano	Georgiopoulou,	Krishnan, Ram
Carbone, Roberto	Zafeiroula	Kuchta, Veronika
Carmichael, Peter	Giannetos, Thanassis	Kunz, Michael
Cha, Sang Gil	Giustolisi, Rosario	Kywe, Su Mon
Chang, Bing	Gottschlich, Wolfram	Köhler, Olaf Markus
Chen, Ping	Grohmann, Bjoern	Lai, Russell W.F.
Chen, Rongmao	Guan, Le	Lancrenon, Jean
Cheng, Yuan	Guanciale, Roberto	Laube, Stefan
Choi, Rakyong	Guarnieri, Marco	Lauer, Sebastian
Chu, Cheng Kang	Gupta, Maanak	Leichter, Carl
Chu, Cheng-Kang	Gyftopoulos, Sotirios	Lerman, Liran
Ciampi, Michele	Hallberg, Sven M.	Li, Depeng
Cianfriglia, Marco	Hallgren, Per	Li, Yan
Clarke, Dylan	Han, Jinguang	Li, Yuping
Cohn-Gordon, Katriel	Hassan, Sabri	Lim, Hoon Wei
Coletta, Alessio	Hauptert, Vincent	Lindemann, Jens
Costa, Gabriele	He, Yongzhong	Lindner, Andreas
Costantino, Gianpiero	Hedin, Daniel	Liu, Jianghua
Cuvelier, Edouard	Henricksen, Matt	Liu, Naiwei

Liu, Ximing	Peroli, Michele	Shirvanian, Maliheh
Liu, Xing	Peters, Thomas	Shojaie, Bahareh
Luhn, Sebastian	Petrovic, Slobodan	Shrestha, Babins
Lyvas, Christos	Pham, Vinh	Shrestha, Prakash
Ma, Jinhua	Pitropakis, Nikolaos	Shulman, Haya
Magkos, Emmanouil	Pridöhl, Henning	Sideri, Maria
Magri, Bernardo	Puchta, Alexander	Siim, Sander
Manoharan, Praveen	Pulls, Tobias	Sjösten, Alexander
Manulis, Mark	Quaglia, Elizabeth	Soria-Comas, Jordi
Marktscheffel, Tobias	Radomirovic, Sasa	Sorniotti, Alessandro
Martinovic, Ivan	Rafnsson, Willard	Sprick, Barbara
Marwah, Manish	Ranise, Silvio	Squarcina, Marco
Marx, Matthias	Rao, Prasad	Stamatelatos, Giorgos
McCorry, Patrick	Reif, Sebastian	Stamatiou, Yannis
Mehrnezhad, Maryam	Reinecke, Philipp	Staudemeyer, Ralf C.
Meng, Weizhi	Rekleitis, Evangelos	Stergiopoulos, George
Merlo, Alessio	Ren, Chuangang	Stütgen, Johannes
Meyer, Maxime	Reuben, Jenni	Su, Dong
Min, Byungho	Rial, Alfredo	Sy, Erik
Moataz, Tarik	Ribeiro De Mello, Emerson	Sänger, Johannes
Mogire, Nancy	Ribes-González, Jordi	Taheri, Somayeh
Mohamed, Manar	Ricci, Sara	Tasch, Markus
Mohammadi, Esfandiar	Richthammer, Hartmut	Tasidou, Aimilia
Montoya, Lorena	Rios, Ruben	Teheri, Somayeh
Moore, Nicholas	Rizomiliotis, Panagiotis	Teixeira, André
Mowbray, Miranda	Rocchetto, Marco	Tempesta, Mauro
Mueller, Johannes	Rochet, Florentin	Thoma, Cory
Mykoniati, Maria	Roenne, Peter	Thompson, Matthew
Mylonas, Alexios	Roth, Christian	Truderung, Tomasz
Möser, Malte	Rothstein Morris, Eric	Tsalis, Nikolaos
Müller, Tilo	Ruan, Na	Tsoumas, Bill
Müller, Tobias	Salas, Julián	Tupakula, Udaya
Nelson, Mark	Saracino, Andrea	Verderame, Luca
Nemati, Hamed	Schmitz, Guido	Virvilis, Nick
Neupane, Ajaya	Schranz, Oliver	Vrakas, Nikos
Nguyen, Binh	Schreckling, Daniel	Walter, Marie-Therese
Nuñez, David	Schöttle, Pascal	Wang, Bolun
Ntantogian, Christoforos	Seidel, Peter-Michael	Wang, Gang
Önen, Melek	Sgandurra, Daniele	Wang, Guilin
Pagnin, Elena	Shafienejad, Masoumeh	Wang, Ruoyu
Palmieri, Paolo	Shah, Ankit	Weber, Alexandra
Panico, Agostino	Shahandashti, Siamak	Weber, Michael
Pankova, Alisa	Sharifian, Setareh	Wei, Zhuo
Park, Jaehong	Sheikhalishahi, Mina	Williams, David
Parra Rodriguez, Juan D.	Shi, Jie	Wolff, Marcus
Parra-Arnau, Javier		Wu, Shuang

Wu, Wei
Wundram, Martin
Wüchner, Tobias
Xiao, Gaoyao
Xing, Xinyu
Xu, Jia
Xu, Ke
Yahia, Muzamil
Yaich, Reda

Yang, Guomin
Yang, Weining
Yautsiukhin, Artsiom
Yerukhimovich, Arkady
Yfantopoulos, Nikos
Yu, Jiangshan
Yu, Xingjie
Yuen, Tsz Hon
Zang, Wanyu

Zavatteri, Matteo
Zerkane, Salaheddine
Zhang, Liang Feng
Zhang, Weiquan
Zhao, Yongjun
Zhou, Lan
Zimmer, Ephraim

Contents – Part I

Network and Web Security

Understanding Cross-Channel Abuse with SMS-Spam Support Infrastructure Attribution	3
<i>Bharat Srinivasan, Payas Gupta, Manos Antonakakis, and Mustaque Ahamad</i>	
Toward an Efficient Website Fingerprinting Defense	27
<i>Marc Juarez, Mohsen Imani, Mike Perry, Claudia Diaz, and Matthew Wright</i>	
Proactive Verification of Security Compliance for Clouds Through Pre-computation: Application to OpenStack	47
<i>Suryadipta Majumdar, Yosr Jarraya, Taous Madi, Amir Alimohammadifar, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi</i>	

Authentication

Comparing Password Ranking Algorithms on Real-World Password Datasets	69
<i>Weining Yang, Ninghui Li, Ian M. Molloy, Youngja Park, and Suresh N. Chari</i>	
Scalable Two-Factor Authentication Using Historical Data	91
<i>Aldar C.-F. Chan, Jun Wen Wong, Jianying Zhou, and Joseph Teo</i>	
On the Implications of Zipf’s Law in Passwords	111
<i>Ding Wang and Ping Wang</i>	

Encrypted Search

PPOPM: More Efficient Privacy Preserving Outsourced Pattern Matching . . .	135
<i>Jun Zhou, Zhenfu Cao, and Xiaolei Dong</i>	
An Efficient Non-interactive Multi-client Searchable Encryption with Support for Boolean Queries	154
<i>Shi-Feng Sun, Joseph K. Liu, Amin Sakzad, Ron Steinfeld, and Tsz Hon Yuen</i>	
Efficient Encrypted Keyword Search for Multi-user Data Sharing	173
<i>Aggelos Kiayias, Ozgur Oksuz, Alexander Russell, Qiang Tang, and Bing Wang</i>	

Detection and Monitoring

Membrane: A Posteriori Detection of Malicious Code Loading by Memory
 Paging Analysis 199
*Gábor Pék, Zsombor Lázár, Zoltán Várnagy, Márk Félegyházi,
 and Levente Buttyán*

Mobile Application Impersonation Detection Using Dynamic
 User Interface Extraction 217
Luka Malisa, Kari Kostainen, Michael Och, and Srdjan Capkun

A Machine Learning Approach for Detecting Third-Party Trackers
 on the Web 238
Qianru Wu, Qixu Liu, Yuqing Zhang, Peng Liu, and Guanxing Wen

Cryptography for Cloud Computing

Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis
 and Optimal Constructions 261
Céline Chevalier, Fabien Laguillaumie, and Damien Vergnaud

Attribute-Based Signatures for Supporting Anonymous Certification 279
Nesrine Kaaniche and Maryline Laurent

Privacy Preserving Computation in Cloud Using Noise-Free Fully
 Homomorphic Encryption (FHE) Schemes 301
Yongge Wang and Qutaibah M. Malluhi

Lightweight Delegatable Proofs of Storage 324
Jia Xu, Anjia Yang, Jianying Zhou, and Duncan S. Wong

Anonymous RAM 344
Michael Backes, Amir Herzberg, Aniket Kate, and Ivan Pryvalov

Efficient Sanitizable Signatures Without Random Oracles 363
*Russell W.F. Lai, Tao Zhang, Sherman S.M. Chow,
 and Dominique Schröder*

Operating Systems Security

Intentio Ex Machina: Android Intent Access Control via an Extensible
 Application Hook 383
Carter Yagemann and Wenliang Du

Hey, You, Get Off of My Image: Detecting Data Residue
 in Android Images 401
Xiao Zhang, Youssa Aafer, Kailiang Ying, and Wenliang Du

NaCIDroid: Native Code Isolation for Android Applications. 422
Elias Athanasopoulos, Vasileios P. Kemerlis, Georgios Portokalidis, and Angelos D. Keromytis

AsyncShock: Exploiting Synchronisation Bugs in Intel SGX Enclaves. 440
Nico Weichbrodt, Anil Kurmus, Peter Pietzuch, and Rüdiger Kapitza

Stay in Your Cage! A Sound Sandbox for Third-Party Libraries on Android. 458
Fabo Wang, Yuqing Zhang, Kai Wang, Peng Liu, and Wenjie Wang

Android Permission Recommendation Using Transitive Bayesian Inference Model 477
Bahman Rashidi, Carol Fung, Anh Nguyen, and Tam Vu

Information Flow

Spot the Difference: Secure Multi-execution and Multiple Facets 501
Nataliia Bielova and Tamara Rezk

On Reductions from Multi-Domain Noninterference to the Two-Level Case . . . 520
Oliver Woizekowski and Ron van der Meyden

Flexible Manipulation of Labeled Values for Information-Flow Control Libraries. 538
Marco Vassena, Pablo Buiras, Lucas Waye, and Alejandro Russo

Software Security

Let’s Face It: Faceted Values for Taint Tracking. 561
Daniel Schoepe, Musard Balliu, Frank Piessens, and Andrei Sabelfeld

IFuzzer: An Evolutionary Interpreter Fuzzer Using Genetic Programming . . . 581
Spandan Veggalam, Sanjay Rawat, Istvan Haller, and Herbert Bos

Automated Multi-architectural Discovery of CFI-Resistant Code Gadgets. . . . 602
Patrick Wollgast, Robert Gawlik, Behrad Garmany, Benjamin Kollenda, and Thorsten Holz

Author Index 621

Contents – Part II

Leakage Management and Obfuscation

Towards Efficient Evaluation of a Time-Driven Cache Attack on Modern Processors	3
<i>Andreas Zankl, Katja Miller, Johann Heyszl, and Georg Sigl</i>	
More Practical and Secure History-Independent Hash Tables	20
<i>Michael T. Goodrich, Evgenios M. Kornaropoulos, Michael Mitzenmacher, and Roberto Tamassia</i>	
On Manufacturing Resilient Opaque Constructs Against Static Analysis.	39
<i>Brendan Sheridan and Micah Sherr</i>	

Secure Multiparty Computation

Robust Password-Protected Secret Sharing	61
<i>Michel Abdalla, Mario Cornejo, Anca Nitulescu, and David Pointcheval</i>	
Compiling Low Depth Circuits for Practical Secure Computation	80
<i>Niklas Buescher, Andreas Holzer, Alina Weber, and Stefan Katzenbeisser</i>	
Secure Computation of MIPS Machine Code	99
<i>Xiao Wang, S. Dov Gordon, Allen McIntosh, and Jonathan Katz</i>	

Secure Logging

Insynd: Improved Privacy-Preserving Transparency Logging	121
<i>Roel Peeters and Tobias Pulls</i>	
Secure Logging Schemes and Certificate Transparency	140
<i>Benjamin Dowling, Felix Günther, Udyani Herath, and Douglas Stebila</i>	

Economics of Security

Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms	161
<i>Aron Laszka, Mingyi Zhao, and Jens Grossklags</i>	
Efficient Numerical Frameworks for Multi-objective Cyber Security Planning	179
<i>MHR. Khouzani, P. Malacaria, C. Hankin, A. Fielder, and F. Smeraldi</i>	

E-voting and E-commerce

On Bitcoin Security in the Presence of Broken Cryptographic Primitives 201
Ilias Giechaskiel, Cas Cremers, and Kasper B. Rasmussen

DRE-ip: A Verifiable E-Voting Scheme Without Tallying Authorities 223
Siamak F. Shahandashti and Feng Hao

When Are Three Voters Enough for Privacy Properties? 241
Myrto Arapinis, Véronique Cortier, and Steve Kremer

Efficient Zero-Knowledge Contingent Payments in Cryptocurrencies
 Without Scripts 261
Wacław Banasik, Stefan Dziembowski, and Daniel Malinowski

Security of the Internet of Things

LeiA: A Lightweight Authentication Protocol for CAN 283
Andreea-Ina Radu and Flavio D. Garcia

Privacy, Discovery, and Authentication for the Internet of Things 301
David J. Wu, Ankur Taly, Asim Shankar, and Dan Boneh

Secure Code Updates for Mesh Networked Commodity Low-End
 Embedded Devices 320
Florian Kohnhäuser and Stefan Katzenbeisser

Authenticated Key Agreement Mediated by a Proxy Re-encryptor
 for the Internet of Things 339
Kim Thuat Nguyen, Nouha Oualha, and Maryline Laurent

Data Privacy

Information Control by Policy-Based Relational Weakening Templates 361
Joachim Biskup and Marcel Preuß

Quantifying Location Privacy Leakage from Transaction Prices 382
*Arthur Gervais, Hubert Ritzdorf, Mario Lucic, Vincent Lenders,
 and Srdjan Capkun*

A Formal Treatment of Privacy in Video Data 406
Valerie Fetzer, Jörn Müller-Quade, and Tobias Nilges

Security of Cyber-Physical Systems

On Attacker Models and Profiles for Cyber-Physical Systems 427
Marco Rocchetto and Nils Ole Tippenhauer

Towards the Automated Verification of Cyber-Physical Security Protocols:
 Bounding the Number of Timed Intruders 450
Vivek Nigam, Carolyn Talcott, and Abraão Aires Urquiza

Safeguarding Structural Controllability in Cyber-Physical Control Systems. . . 471
Cristina Alcaraz and Javier Lopez

Attacks

The Beauty or The Beast? Attacking Rate Limits of the Xen Hypervisor 493
Johanna Ullrich and Edgar Weippl

Autocomplete Injection Attack 512
Nethanel Gelernter and Amir Herzberg

Breaking into the KeyStore: A Practical Forgery Attack
 Against Android KeyStore 531
Mohamed Sabt and Jacques Traorè

Attribute-Based Cryptography

Traceable CP-ABE with Short Ciphertexts: How to Catch People Selling
 Decryption Devices on eBay Efficiently. 551
Jianting Ning, Zhenfu Cao, Xiaolei Dong, Junqing Gong, and Jie Chen

Server-Aided Revocable Attribute-Based Encryption 570
Hui Cui, Robert H. Deng, Yingjiu Li, and Baodong Qin

Online/Offline Public-Index Predicate Encryption for Fine-Grained Mobile
 Access Control 588
Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, and Kaitai Liang

Author Index 607