

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>

Simon N. Foley · Dieter Gollmann
Einar Snekkenes (Eds.)

Computer Security – ESORICS 2017

22nd European Symposium on Research in Computer Security
Oslo, Norway, September 11–15, 2017
Proceedings, Part II

Editors

Simon N. Foley
IMT Atlantique
Rennes
France

Einar Snekkenes
NTNU
Gjøvik
Norway

Dieter Gollmann
Hamburg University of Technology
Hamburg
Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-66398-2 ISBN 978-3-319-66399-9 (eBook)
DOI 10.1007/978-3-319-66399-9

Library of Congress Control Number: 2017949525

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book contains the papers that were selected for presentation and publication at the 22nd European Symposium on Research in Computer Security, ESORICS 2017, which was held in Oslo, Norway, September 11–15, 2017. The aim of ESORICS is to further the progress of research in computer security by bringing together researchers in the area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

The Program Committee accepted 54 papers out of a total of 338 papers that were submitted from 51 different countries, resulting in an acceptance rate of 16%. The accepted papers are drawn from a wide range of topics, including data protection, security protocols, systems, web and network security, privacy, threat modelling and detection, information flow and security in emerging applications such as cryptocurrencies, the Internet of Things, and automotive. The 120-member Program Committee, assisted by a further 334 external reviewers, reviewed and discussed the papers online over a period of 8 weeks, writing a total of 1015 reviews for authors.

ESORICS 2017 would not have been possible without the contributions of the many volunteers who freely gave their time and expertise. We would like to thank the members of the Program Committee and the external reviewers for their substantial work in evaluating the papers. We would also like to thank the ESORICS Steering Committee and its Chair Pierangela Samarati; the Organisation Chair Laura Georg; the Publicity Chair Cristina Alcaraz; the Workshop Chair Sokratis Katsikas and all workshop co-chairs, who organized the workshops co-located with ESORICS. We would like to especially thank the sponsors of this year's ESORICS conference: the Center for Cyber and Information Security, COINS Research School, KPMG, the Norwegian University of Science and Technology NTNU, Oxford University Press, and the Research Council of Norway.

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

July 2017

Simon Foley
Dieter Gollmann
Einar Snekkenes

Organization

Program Committee

Gail-Joon Ahn	Arizona State University, USA
Alessandro Armando	University of Genoa and Fondazione Bruno Kessler, Italy
Frederik Armknecht	Universität Mannheim, Germany
Michael Backes	CISPA, Saarland University, Germany
Giampaolo Bella	Università di Catania, Italy
Zinaida Benenson	University of Erlangen-Nuremberg, Germany
Elisa Bertino	Purdue University, USA
Carlo Blundo	Università degli Studi di Salerno, Italy
Rainer Boehme	University of Innsbruck, Austria
Colin Boyd	Norwegian University of Science and Technology (NTNU), Norway
Stefan Brunthaler	Paderborn University, Germany
Chris Brzuska	TU Hamburg, Germany
Tom Chothia	University of Birmingham, UK
Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong, China
Mauro Conti	University of Padua, Italy
Cas Cremers	University of Oxford, UK
Frédéric Cuppens	IMT Atlantique, France
Nora Cuppens-Boulahia	IMT Atlantique, 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
Wenliang Du	Syracuse University, USA
Pavlos Efraimidis	Democritus University of Thrace, Greece
Hannes Federrath	University of Hamburg, Germany
Simone Fischer-Hübner	Karlstad University, Sweden
Riccardo Focardi	Università Ca' Foscari, Venice, Italy
Simon Foley	IMT Atlantique, France
Sara Foresti	DI - Università degli Studi di Milano, Italy
Felix Freiling	Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany
Sibylle Froeschle	University of Oldenburg, Germany
Lenzini Gabriele	SnT/University of Luxembourg, Luxembourg
Joaquin Garcia-Alfaro	Télécom SudParis, France
Dieter Gollmann	TU Hamburg, Germany

Dimitris Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Joshua Guttman	Worcester Polytechnic Institute, USA
Gerhard Hancke	City University of Hong Kong, Hong Kong, China
Marit Hansen	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany
Rene Rydhof Hansen	Aalborg University, Denmark
Feng Hao	Newcastle University, UK
Cormac Herley	Microsoft Research, USA
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
Limin Jia	Carnegie Mellon University, USA
Wouter Joosen	Katholieke Universiteit Leuven, Belgium
Vasilis Katos	Bournemouth University, UK
Sokratis Katsikas	Center for Cyber and Information Security, NTNU, Norway
Florian Kerschbaum	University of Waterloo, Canada
Dogan Kesdogan	Universität Regensburg, Germany
Kwangjo Kim	KAIST, South Korea
Steve Kremer	Inria Nancy - Grand Est, France
Marina Krotofil	Honeywell Industrial Cyber Security Lab, USA
Ralf Küsters	University of Stuttgart, Germany
Junzuo Lai	Singapore Management University, Singapore
Kwok Yan Lam	Nanyang Technological University, Singapore
Costas Lambrinouidakis	University of Piraeus, Greece
Peeter Laud	Cybernetica AS, Estonia
Adam J. Lee	University of Pittsburgh, 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 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
Sjouke Mauw	University of Luxembourg, Luxembourg
Antonio Maña	University of Malaga, Spain
Catherine Meadows	NRL, USA
John Mitchell	Stanford University, USA
Aikaterini Mitrokotsa	Chalmers University of Technology, Sweden
Refik Molva	EURECOM, France
Charles Morisset	Newcastle University, UK
Rolf Oppliger	eSECURITY Technologies, Switzerland

Stefano Paraboschi	Università di Bergamo, Italy
Dusko Pavlovic	University of Hawaii, USA
Günther Pernul	Universität Regensburg, Germany
David Pichardie	ENS Rennes/IRISA/Inria, France
Frank Piessens	Katholieke Universiteit Leuven, Belgium
Wolter Pieters	Delft University of Technology, The Netherlands
Michalis Polychronakis	Stony Brook University, USA
Joachim Posegga	University of Passau, Germany
Christian W. Probst	Technical University of Denmark, Denmark
Christina Pöpper	New York University Abu Dhabi, UAE
Kai Rannenberg	Goethe University Frankfurt, Germany
Awais Rashid	Lancaster University, UK
Indrajit Ray	Colorado State University, USA
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
Reyhaneh 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	Verified IO Limited
Einar Snekkenes	NTNU, Norway
Willy Susilo	University of Wollongong, Australia
Krzysztof Szczypiorski	Warsaw University of Technology, Poland
Björn Tackmann	IBM Research, Switzerland
Qiang Tang	Cornell University, USA
Nils Ole Tippenhauer	Singapore University of Technology and Design, Singapore
Aggeliki Tsohou	Ionian University, Greece
Jaideep Vaidya	Rutgers University, USA
Vijay Varadharajan	The University of Newcastle, UK
Luca Viganò	King's College London, UK
Michael Waidner	Fraunhofer SIT, Germany
Cong Wang	City University of Hong Kong, Hong Kong, China
Lingyu Wang	Concordia University, USA
Edgar Weippl	SBA Research, Austria
Stephen D. Wolthusen	Royal Holloway, University of London, UK and Norwegian University of Science and Technology, Norway
Christos Xenakis	University of Piraeus, Greece

Jeff Yan	Lancaster University, UK
Meng Yu	University of Texas at San Antonio, USA
Ben Zhao	University of Chicago, USA
Jianying Zhou	Singapore University of Technology and Design, Singapore
Haojin Zhu	Shanghai Jiao Tong University, China

Additional Reviewers

Abdullah, Lamya	Blanc, Gregory
Abramova, Svetlana	Blanco-Justicia, Alberto
Agudo, Isaac	Blochberger, Maximilian
Ah-Fat, Patrick	Bogaerts, Jasper
Ahlawat, Amit	Boschini, Cecilia
Akowuah, Francis	Bossen, Jannek Alexander Westerhof
Albanese, Massimiliano	Boureau, Ioana
Alimohammadifar, Amir	Bours, Patrick
Alpirez Bock, Estuardo	Brandt, Markus
Alrabae, Saed	Brooks, Tyson
Ambrosin, Moreno	Bruni, Alessandro
Aminanto, Muhamad Erza	Buhov, Damjan
Anand, S Abhishek	Bullee, Jan-Willem
Angles-Tafalla, Carles	Burkert, Christian
Aonzo, Simone	Bursuc, Sergiu
Arlitt, Martin	Busch, Marcel
Arriaga, Afonso	Butin, Denis
Assaf, Mounir	Böhm, Fabian
Atzeni, Andrea	Calzavara, Stefano
Auerbach, Benedikt	Carmichael, Peter
Avizheh, Sepideh	Ceccato, Mariano
Bacis, Enrico	Chen, Jie
Bag, Samiran	Chen, Long
Bajramovic, Edita	Chen, Rongmao
Ban Kirigin, Tajana	Cheng, Peng
Barber, Simon	Cheval, Vincent
Bardin, Sebastien	Choi, Rakyong
Bastys, Iulia	Ciampi, Michele
Basu, Hridam	Clark, Daniel
Baumann, Christoph	Cohn-Gordon, Katriel
Belgacem, Boutheyna	Costa, Gabriele
Berbecaru, Diana	Costache, Anamaria
Besson, Frédéric	Costantino, Gianpiero
Bilzhause, Arne	Courtois, Nicolas
Biondi, Fabrizio	Dai, Tianxiang
Bkakria, Anis	Dantas, Yuri Gil

Davies, Gareth T.
De Benedictis, Marco
De Gaspari, Fabio
De Meo, Federico
Dehnel-Wild, Martin
Del Pino, Rafaël
Desmet, Lieven
Drogkaris, Prokopios
Drosatos, George
Duman, Onur
Duong, Tuyet
Fan, Xiong
Farràs, Oriol
Fernandez, Carmen
Ferrari, Stefano
Fett, Daniel
Fleischhacker, Nils
Freeman, Kevin
Frey, Sylvain
Gadyatskaya, Olga
Garratt, Luke
Gazeau, Ivan
Genc, Ziya A.
Geneiatakis, Dimitris
Georgiopolou, Zafeiroula
Gervais, Arthur
Giustolisi, Rosario
Gogioso, Stefano
Gonzalez-Burgueño, Antonio
Gritti, Clémentine
Groll, Sebastian
Grosz, Akos
Guan, Le
Guanciaale, Roberto
Gunasinghe, Hasini
Gyftopoulos, Sotirios
Gérard, François
Götzfried, Johannes
Hallgren, Per
Hamann, Tobias
Hammann, Sven
Han, Jinguang
Harborth, David
Hartmann, Lukas
Hassan, Sabri
Hatamian, Majid
Hauptert, Vincent
Hausknecht, Daniel
Herrera, Jordi
Hils, Maximilian
Huang, Yi
Hummer, Matthias
Ilia, Panagiotis
Iovino, Vincenzo
Islam, Morshed
Issel, Katharina
Iwaya, Leonardo
Jackson, Dennis
Jansen, Kai
Jansen, Rob
Jhawar, Ravi
Joensen, Ólavur Debes
Johannes, Schickel
Jonker, Hugo
Jourdan, Jacques-Henri
Jäschke, Angela
Kalloniatis, Christos
Kandias, Miltiadis
Katz, Jonathan
Kerstan, Henning
Kersten, Rody
Kintis, Panagiotis
Kohls, Katharina
Kokolakis, Spyros
Kountouras, Athanasios
Kuchta, Veronika
Kälber, Sven
Köstler, Johannes
Labunets, Katsiaryna
Lacoste, Marc
Lagorio, Giovanni
Lai, Russell W.F.
Lain, Daniele
Lal, Chhagan
Laperdrix, Pierre
Laporte, Vincent
Latz, Tobias
Lazrig, Ibrahim
Learney, Robert
Lehmann, Anja
Leontiadis, Iraklis
Li, Hanyi

Li, Ximeng
 Liang, Kaitai
 Lin, Fuchun
 Liu, Ximeng
 Liu, Ximing
 Lochbihler, Andreas
 Lopez, Jose M.
 Lu, Yuan
 Lyvas, Christos
 Ma, Jack P.K.
 Mace, John
 Madi, Taous
 Magkos, Emmanouil
 Mahgoub Yahia Mohamed, Muzamil
 Majumdar, Suryadipta
 Maragoudakis, Manolis
 Marino, Francesco
 Marktscheffel, Tobias
 Martinez, Sergio
 Marx, Matthias
 Mateus, Paulo
 McEvoy, Richard
 Mehnaz, Shagufta
 Melicher, William
 Mercaldo, Francesco
 Meyer, Maxime
 Mizera, Andrzej
 Momeni, Sadaf
 Moore, Nicholas
 Muehlberg, Jan Tobias
 Müller, Johannes
 Mukherjee, Subhojeet
 Mulamba, Dieudonne
 Mylonas, Alexios
 Navarro-Arribas, Guillermo
 Nemati, Hamed
 Neupane, Ajaya
 Neven, Gregory
 Nieto, Ana
 Ntouskas, Teo
 Nuñez, David
 Olesen, Anders Trier
 Oqaily, Momen
 Ordean, Mihai
 Önen, Melek
 Palmarini, Francesco
 Pang, Jun
 Panico, Agostino
 Parra-Arnau, Javier
 Pasquini, Cecilia
 Patachi, Stefan
 Pelosi, Gerardo
 Petit, Christophe
 Petrovic, Slobodan
 Pham, Vinh
 Pitropakis, Nikolaos
 Preuveneers, Davy
 Pridöhl, Henning
 Puchta, Alexander
 Pulls, Tobias
 Pérez-Solà, Cristina
 Rafnsson, Willard
 Rajagopalan, Siva
 Rakotondravony, Noelle
 Rao, Fang-Yu
 Rausch, Daniel
 Rekleitis, Evangelos
 Reuben, Jenni
 Ribes-González, Jordi
 Ricci, Sara
 Richthammer, Hartmut
 Rios, Ruben
 Rosa, Marco
 Roth, Christian
 Roux-Langlois, Adeline
 Rupprecht, David
 Saracino, Andrea
 Satvat, Kiavash
 Saxena, Neetesh
 Schiffman, Joshua
 Schmid, Lara
 Schmitz, Christopher
 Schmitz, Guido
 Schneider, David
 Schnitzler, Theodor
 Schoepe, Daniel
 Schoettle, Pascal
 Schroeder, Dominique
 Schwarz, Oliver
 Sciarretta, Giada
 Senf, Daniel
 Sgandurra, Daniele

Shah, Ankit
Shahandashti, Siamak
Sheikhalishahi, Mina
Shen, Jian
Shirani, Paria
Shirvanian, Maliheh
Shrestha, Prakash
Shulman, Haya
Simo, Hervais
Siniscalchi, Luisa
Sjösten, Alexander
Skrobot, Marjan
Smith, Geoffrey
Soria-Comas, Jordi
Soska, Kyle
Spolaor, Riccardo
Stamatelatos, Giorgos
Stergiopoulos, George
Strackx, Raoul
Stübs, Marius
Su, Tao
Sy, Erik
Sänger, Johannes
Tai, Raymond K.H.
Tasch, Markus
Tasidou, Aimilia
Taubmann, Benjamin
Taylor, Gareth
Tesfay, Welderufael
Tolomei, Gabriele
Truderung, Tomasz
Trujillo, Rolando
Tsalis, Nikolaos
Tupakula, Uday
Vallini, Marco
Van Acker, Steven
Van Bulck, Jo
van Ginkel, Neline
Van Rompay, Cédric
Vanbrabant, Bart
Vasilopoulos, Dimitrios
Vazquez Sandoval, Itzel
Venkatesan, Sridhar
Venturi, Daniele
Veseli, Fatbardh
Vielberth, Manfred
Virvilis, Nick
Vissers, Thomas
Volkamer, Melanie
Wang, Jiafan
Wang, Minqian
Wang, Qinglong
Wang, Wei
Wang, Xiuhua
Weber, Alexandra
Weber, Michael
Wikström, Douglas
Wolter, Katinka
Wong, Harry W.H.
Woo, Maverick
Xu, Jun
Xu, Ke
Xu, Peng
Yaich, Reda
Yang, S.J.
Yautsiukhin, Artsiom
Yesuf, Ahmed Seid
Ying, Kailiang
Yu, Jiangshan
Yu, Xingjie
Zamyatin, Alexei
Zavatteri, Matteo
Zhang, Liang Feng
Zhang, Mengyuan
Zhang, Yuqing
Zhao, Yongjun
Zhao, Yunwei
Zhou, Lan
Zhu, Fei
Ziener, Daniel
Zimmer, Ephraim

Contents – Part II

Automated Analysis of Equivalence Properties for Security Protocols Using Else Branches	1
<i>Ivan Gazeau and Steve Kremer</i>	
Quantifying Web Adblocker Privacy	21
<i>Arthur Gervais, Alexandros Filios, Vincent Lenders, and Srdjan Capkun</i>	
More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds	43
<i>Essam Ghadafi</i>	
Adversarial Examples for Malware Detection	62
<i>Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, and Patrick McDaniel</i>	
PerfWeb: How to Violate Web Privacy with Hardware Performance Events.	80
<i>Berk Gulmezoglu, Andreas Zankl, Thomas Eisenbarth, and Berk Sunar</i>	
Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise (‘DiskFiltration’)	98
<i>Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici</i>	
DOMPurify: Client-Side Protection Against XSS and Markup Injection	116
<i>Mario Heiderich, Christopher Späth, and Jörg Schwenk</i>	
Preventing DNS Amplification Attacks Using the History of DNS Queries with SDN.	135
<i>Soyoung Kim, Sora Lee, Geumhwan Cho, Muhammad Ejaz Ahmed, Jaehoon (Paul) Jeong, and Hyoungshick Kim</i>	
A Traceability Analysis of Monero’s Blockchain.	153
<i>Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena</i>	
Multi-rate Threshold FlipThem	174
<i>David Leslie, Chris Sherfield, and Nigel P. Smart</i>	
Practical Keystroke Timing Attacks in Sandboxed JavaScript	191
<i>Moritz Lipp, Daniel Gruss, Michael Schwarz, David Bidner, Clémentine Maurice, and Stefan Mangard</i>	
On-Demand Time Blurring to Support Side-Channel Defense.	210
<i>Weijie Liu, Debin Gao, and Michael K. Reiter</i>	

VuRLE: Automatic Vulnerability Detection and Repair by Learning from Examples	229
<i>Siqi Ma, Ferdian Thung, David Lo, Cong Sun, and Robert H. Deng</i>	
Link-Layer Device Type Classification on Encrypted Wireless Traffic with COTS Radios	247
<i>Rajib Ranjan Maiti, Sandra Siby, Ragav Sridharan, and Nils Ole Tippenhauer</i>	
LeaPS: Learning-Based Proactive Security Auditing for Clouds	265
<i>Suryadipta Majumdar, Yosr Jarraya, Momen Oqaily, Amir Alimohammadifar, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi</i>	
Identifying Multiple Authors in a Binary Program.	286
<i>Xiaozhu Meng, Barton P. Miller, and Kwang-Sung Jun</i>	
Secure IDS Offloading with Nested Virtualization and Deep VM Introspection	305
<i>Shohei Miyama and Kenichi Kourai</i>	
Privacy Implications of Room Climate Data	324
<i>Philipp Morgner, Christian Müller, Matthias Ring, Björn Eskofier, Christian Riess, Frederik Armknecht, and Zinaida Benenson</i>	
Network Intrusion Detection Based on Semi-supervised Variational Auto-Encoder.	344
<i>Genki Osada, Kazumasa Omote, and Takashi Nishide</i>	
No Sugar but All the Taste! Memory Encryption Without Architectural Support	362
<i>Panagiotis Papadopoulos, Giorgos Vasiliadis, Giorgos Christou, Evangelos Markatos, and Sotiris Ioannidis</i>	
Inference-Proof Updating of a Weakened View Under the Modification of Input Parameters	381
<i>Joachim Biskup and Marcel Preuß</i>	
Preventing Advanced Persistent Threats in Complex Control Networks	402
<i>Juan E. Rubio, Cristina Alcaraz, and Javier Lopez</i>	
Shortfall-Based Optimal Placement of Security Resources for Mobile IoT Scenarios	419
<i>Antonino Rullo, Edoardo Serra, Elisa Bertino, and Jorge Lobo</i>	

Boot Attestation: Secure Remote Reporting with Off-The-Shelf
 IoT Sensors 437
*Steffen Schulz, André Schaller, Florian Kohnhäuser,
 and Stefan Katzenbeisser*

RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature)
 Protocol for Blockchain Cryptocurrency Monero. 456
Shi-Feng Sun, Man Ho Au, Joseph K. Liu, and Tsz Hon Yuen

SePCAR: A Secure and Privacy-Enhancing Protocol
 for Car Access Provision 475
*Iraklis Symeonidis, Abdelrahman Aly, Mustafa Asan Mustafa,
 Bart Mennink, Siemen Dhooghe, and Bart Preneel*

Privacy-Preserving Decision Trees Evaluation via Linear Functions. 494
*Raymond K.H. Tai, Jack P.K. Ma, Yongjun Zhao,
 and Sherman S.M. Chow*

Stringer: Measuring the Importance of Static Data Comparisons
 to Detect Backdoors and Undocumented Functionality. 513
Sam L. Thomas, Tom Chothia, and Flavio D. Garcia

Generic Constructions for Fully Secure Revocable
 Attribute-Based Encryption. 532
*Kotoko Yamada, Nuttapong Attrapadung, Keita Emura,
 Goichiro Hanaoka, and Keisuke Tanaka*

Enforcing Input Correctness via Certification in Garbled
 Circuit Evaluation 552
Yihua Zhang, Marina Blanton, and Fattaneh Bayatbabolghani

Author Index 571

Contents – Part I

From Intrusion Detection to Software Design	1
<i>Sandro Etalle</i>	
Justifying Security Measures — a Position Paper	11
<i>Cormac Herley</i>	
The Once and Future Onion	18
<i>Paul Syverson</i>	
Tightly Secure Ring-LWE Based Key Encapsulation with Short Ciphertexts	29
<i>Martin R. Albrecht, Emmanuela Orsini, Kenneth G. Paterson, Guy Peer, and Nigel P. Smart</i>	
Tree-Based Cryptographic Access Control	47
<i>James Alderman, Naomi Farley, and Jason Crampton</i>	
Source Code Authorship Attribution Using Long Short-Term Memory Based Networks	65
<i>Bander Alsulami, Edwin Dauber, Richard Harang, Spiros Mancoridis, and Rachel Greenstadt</i>	
Is My Attack Tree Correct?	83
<i>Maxime Audinot, Sophie Pinchinat, and Barbara Kordy</i>	
Server-Aided Secure Computation with Off-line Parties	103
<i>Foteini Baldimtsi, Dimitrios Papadopoulos, Stavros Papadopoulos, Alessandra Scafuro, and Nikos Triandopoulos</i>	
We Are Family: Relating Information-Flow Trackers	124
<i>Musard Balliu, Daniel Schoepe, and Andrei Sabelfeld</i>	
Labeled Homomorphic Encryption: Scalable and Privacy-Preserving Processing of Outsourced Data	146
<i>Manuel Barbosa, Dario Catalano, and Dario Fiore</i>	
MTD CBITS: Moving Target Defense for Cloud-Based IT Systems	167
<i>Alexandru G. Bardas, Sathya Chandran Sundaramurthy, Xinming Ou, and Scott A. DeLoach</i>	
Modular Verification of Protocol Equivalence in the Presence of Randomness	187
<i>Matthew S. Bauer, Rohit Chadha, and Mahesh Viswanathan</i>	

Non-interactive Provably Secure Attestations for Arbitrary RSA Prime Generation Algorithms	206
<i>Fabrice Benhamouda, Houda Ferradi, Rémi Géraud, and David Naccache</i>	
Reusing Nonces in Schnorr Signatures: (and Keeping It Secure...)	224
<i>Marc Beunardeau, Aisling Connolly, Houda Ferradi, Rémi Géraud, David Naccache, and Damien Vergnaud</i>	
WebPol: Fine-Grained Information Flow Policies for Web Browsers	242
<i>Abhishek Bichhawat, Vineet Rajani, Jinank Jain, Deepak Garg, and Christian Hammer</i>	
Verifying Constant-Time Implementations by Abstract Interpretation	260
<i>Sandrine Blazy, David Pichardie, and Alix Trieu</i>	
Mirage: Toward a Stealthier and Modular Malware Analysis Sandbox for Android	278
<i>Lorenzo Bordonni, Mauro Conti, and Riccardo Spolaor</i>	
Zero Round-Trip Time for the Extended Access Control Protocol	297
<i>Jacqueline Brendel and Marc Fischlin</i>	
Server-Supported RSA Signatures for Mobile Devices	315
<i>Ahto Buldas, Aivo Kalu, Peeter Laud, and Mart Oruaas</i>	
Verifiable Document Redacting	334
<i>Hervé Chabanne, Rodolphe Hugel, and Julien Keuffner</i>	
Securing Data Analytics on SGX with Randomization	352
<i>Swarup Chandra, Vishal Karande, Zhiqiang Lin, Latifur Khan, Murat Kantarcioglu, and Bhavani Thuraisingham</i>	
DeltaPhish: Detecting Phishing Webpages in Compromised Websites	370
<i>Igino Corona, Battista Biggio, Matteo Contini, Luca Piras, Roberto Corda, Mauro Mereu, Guido Mureddu, Davide Ariu, and Fabio Roli</i>	
Secure Authentication in the Grid: A Formal Analysis of DNP3: SAV5	389
<i>Cas Cremers, Martin Dehnel-Wild, and Kevin Milner</i>	
Per-Session Security: Password-Based Cryptography Revisited	408
<i>Grégory Demay, Peter Gazi, Ueli Maurer, and Björn Tackmann</i>	
AVR Processors as a Platform for Language-Based Security	427
<i>Florian Dewald, Heiko Mantel, and Alexandra Weber</i>	

A Better Composition Operator for Quantitative Information	446
Flow Analyses	446
<i>Kai Engelhardt</i>	
Analyzing the Capabilities of the CAN Attacker	464
<i>Sibylle Fröschle and Alexander Stühling</i>	
Erratum to: Per-Session Security: Password-Based	
Cryptography Revisited	E1
<i>Grégory Demay, Peter Gaži, Ueli Maurer, and Björn Tackmann</i>	
Author Index	483