

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

Jason Crampton Sushil Jajodia
Keith Mayes (Eds.)

Computer Security – ESORICS 2013

18th European Symposium
on Research in Computer Security
Egham, UK, September 9-13, 2013
Proceedings



Springer

Volume Editors

Jason Crampton
Royal Holloway, University of London
Information Security Group
Egham Hill, Egham, TW20 0EX, UK
E-mail: jason.crampton@rhul.ac.uk

Sushil Jajodia
George Mason University
Center for Secure Information Systems
4400 University Drive, Fairfax, VA 22030-4422, USA
E-mail: jajodia@gmu.edu

Keith Mayes
Royal Holloway, University of London
Information Security Group
Egham Hill, Egham, TW20 0EX, UK
E-mail: keith.mayes@rhul.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-40202-9 e-ISBN 978-3-642-40203-6
DOI 10.1007/978-3-642-40203-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013944563

CR Subject Classification (1998): K.6.5, E.3, D.4.6, K.4.4, C.2.0, J.1, H.2.7

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2013

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

This volume contains the papers selected for presentation at the 18th European Symposium on Research in Computer Security (ESORICS 2013), held during September 9–13, 2013, in Egham, UK.

In response to the symposium’s call for papers, 242 papers were submitted to the conference from 38 countries. These papers 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.

The Program Committee’s work was carried out electronically, yielding intensive discussions over a period of a few weeks. Of the papers submitted, 43 were selected for presentation at the conference (resulting in an acceptance rate of 18%). We note that many top-quality submissions were not selected for presentation because of the high technical level of the overall submissions, and we are certain that many of these submissions will, nevertheless, be published at other competitive forums in the future.

An event like ESORICS 2013 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. 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; Sheila Cobourne, for maintaining the website; and the Local Organizing Committee, for helping with organization and taking care of local arrangements. We would also like to express our appreciation to everyone who organized the workshops (CATACRYPT, Cryptoforma, DPM, EUROPKI, QASA, SETOP, STM, Trustworthy Clouds) co-located with ESORICS. A number of organizations also deserve special thanks, including Royal Holloway University of London for acting as host, and the ESORICS sponsors: CESG, Transport for London, ISG Smart Card Centre, Crisp Telecom Limited, and NESSoS.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the symposium’s attendees. We hope you find the proceedings of ESORICS 2013 stimulating and a source of inspiration for your future research and education programs.

September 2013

Jason Crampton
Sushil Jajodia
Keith Mayes

Organization

General Chair

Keith Mayes	Royal Holloway, University of London, UK
-------------	--

Program Chairs

Jason Crampton	Royal Holloway, University of London, UK
Sushil Jajodia	George Mason University, USA

ESORICS Steering Committee

Michael Backes	Saarland University, Germany
Joachim Biskup	University of Dortmund, Germany
Frédéric Cuppens	Télécom Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Yves Deswarte	LAAS, France
Dieter Gollmann	TU Hamburg-Harburg, Germany
Sokratis Katsikas	University of Piraeus, Greece
Mirosław Kutylowski	Wrocław University of Technology, Poland
Javier Lopez	University of Malaga, Spain
Jean-Jacques Quisquater	UCL Crypto Group, Belgium
Peter Ryan	University of Luxembourg, Luxembourg
Pierangela Samarati (Chair)	Università degli Studi di Milano, Italy
Einar Snekkenes	Gjøvik University College, Norway
Michael Waidner	TU Darmstadt, Germany

Publicity Chair

Giovanni Livraga	Università degli Studi di Milano, Italy
------------------	---

Local Organizing Committee

Geraint Price	Royal Holloway, University of London, UK
Gerhard Hancke	Royal Holloway, University of London, UK
Kostas Markantonakis	Royal Holloway, University of London, UK
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Sheila Cobourne	Royal Holloway, University of London, UK

Emma Mosley
Jenny Lee

Royal Holloway, University of London, UK
Royal Holloway, University of London, UK

Program Committee

Gail-Joon Ahn
Massimiliano Albanese
Claudio Agostino Ardagna
Alessandro Armando
Michael Backes

David Basin
Kevin Bauer
Lujo Bauer
Konstantin Beznosov
Marina Blanton
Carlo Blundo
Kevin Butler
Srdjan Capkun
Liqun Chen
Sherman S.M. Chow
Marco Cova
Jason Crampton
Frédéric Cuppens
Sabrina De Capitani

Di Vimercati
Roberto Di Pietro
Claudia Diaz
Josep Domingo-Ferrer
Wenliang Du
Riccardo Focardi
Simon Foley
Sara Foresti
Cedric Fournet
Keith Frikken
Dieter Gollmann
Dimitris Gritzalis

Gerhard Hancke
Amir Herzberg
Michael Huth
Sushil Jajodia
Aaron Johnson
Jonathan Katz
Stefan Katzenbeisser
Engin Kirda

Arizona State University, USA
George Mason University, USA
Università degli Studi di Milano, Italy
University of Genova, Italy
Saarland University and Max Planck Institute
for Software Systems, Germany
ETH Zurich, Switzerland
MIT Lincoln Laboratory, USA
Carnegie Mellon University, USA
UBC, Canada
University of Notre Dame, USA
Università di Salerno, Italy
University of Oregon, USA
ETH Zurich, Switzerland
Hewlett-Packard Laboratories, UK
Chinese University of Hong Kong, SAR China
University of Birmingham, UK
Royal Holloway, University of London, UK
TELECOM Bretagne, France

Università degli Studi di Milano, Italy
Università di Roma Tre, Italy
K.U. Leuven, Belgium
Rovira i Virgili University, Spain
Syracuse University, USA
Università Ca' Foscari di Venezia, Italy
University College Cork, Ireland
Università degli Studi di Milano, Italy
Microsoft, UK
Miami University, USA
Hamburg University of Technology, Germany
Athens University of Economics and Business,
Greece
Royal Holloway, University of London, UK
Bar Ilan University, Israel
Imperial College London, UK
George Mason University, USA
Naval Research Laboratory, USA
University of Maryland, USA
TU Darmstadt, Germany
Northeastern University, USA

Markulf Kohlweiss	Microsoft Research Cambridge, UK
Steve Kremer	INRIA Nancy - Grand Est, France
Mirosław Kutylowski	Wrocław University of Technology, Poland
Adam J. Lee	University of Pittsburgh, USA
Wenke Lee	Georgia Institute of Technology, USA
Yingjiu Li	Singapore Management University, Singapore
Benoit Libert	Technicolor, France
Javier Lopez	University of Malaga, Spain
Wenjing Lou	Virginia Polytechnic Institute and State University, USA
Pratyusa K Manadhata	HP Labs, USA
Luigi Mancini	Università di Roma La Sapienza, Italy
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Gregory Neven	IBM Zurich Research Laboratory, Switzerland
Stefano Paraboschi	Università di Bergamo, Italy
Kenneth Paterson	Royal Holloway, University of London, UK
Dusko Pavlovic	Royal Holloway, University of London, UK
Günther Pernul	Universität Regensburg, Germany
Frank Piessens	Katholieke Universiteit Leuven, Belgium
Michalis Polychronakis	Columbia University, USA
Alexander Pretschner	Technische Universität München, Germany
Kui Ren	State University of New York at Buffalo, USA
Mark Ryan	University of Birmingham, UK
P.Y.A. Ryan	University of Luxembourg, Luxembourg
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Ahmad-Reza Sadeghi	TU Darmstadt, Germany
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Radu Sion	Stony Brook University, USA
Nigel Smart	University of Bristol, UK
Einar Sneekenes	Gjøvik University College, Norway
Vipin Swarup	The MITRE Corporation, USA
Roberto Tamassia	Brown University, USA
Carmela Troncoso	IBBT-K.U.Leuven, ESAT/COSIC, Belgium
Yevgeniy Vahlis	University of Toronto, Canada
Jaideep Vaidya	Rutgers University, USA
Vijay Varadharajan	Macquarie University, Australia
Venkat Venkatakrishnan	University of Illinois at Chicago, USA
Luca Viganò	University of Verona, Italy
Michael Waidner	Fraunhofer SIT, Germany
Bogdan Warinschi	University of Bristol, USA
Ting Yu	North Carolina State University, USA
Moti Yung	Google and Columbia University, USA

Additional Reviewers

Ahmadi, Ahmad
 Alfardan, Nadhem
 Aliasgari, Mehrdad
 Alimomeni, Mohsen
 Androulaki, Elli
 Arriaga, Afonso
 Asharov, Gilad
 Balsa, Ero
 Banescu, Sebastian
 Basu, Anirban
 Batten, Ian
 Baum, Carsten
 Beato, Filipe
 Ben Hamouda, Fabrice
 Bertolissi, Clara
 Bkakra, Anis
 Blaskiewicz, Przemyslaw
 Boyd, Colin
 Bozzato, Claudio
 Broser, Christian
 Brzuska, Christina
 Cachin, Christian
 Calvi, Alberto
 Calzavara, Stefano
 Carbone, Roberto
 Catalano, Dario
 Chandran, Nishanth
 Chen, Jiageng
 Chen, Ling
 Chen, Si
 Chen, Xihui
 Cheval, Vincent
 Choo, Euijin
 Collberg, Christian
 Cremers, Cas
 Cuppens-Boulahia, Nora
 Datta, Anupam
 De Benedictis, Alessandra
 De Caro, Angelo
 De Groef, Willem
 De Ryck, Philippe
 Del Tedesco, Filippo
 Delaune, Stéphanie

Devriese, Dominique
 Du, Changlai
 Durgin, Nancy
 Epasto, Alessandro
 Farnan, Nicholas
 Farràs, Oriol
 Ferdman, Mike
 Fernandez-Gago, Carmen
 Fitzgerald, William Michael
 Frank, Mario
 Fromm, Alexander
 Fuchs, Andreas
 Fuchs, Ludwig
 Futa, Yuichi
 Gajek, Sebastian
 Galbraith, Steven
 Galindo, David
 Garrison, William
 Gasti, Paolo
 Gelernter, Nethanel
 George, Wesley
 Ghiglieri, Marco
 Gilad, Yossi
 Giustolisi, Rosario
 Gjomemo, Rigel
 Goberman, Michael
 Grewal, Gurchetan S.
 Hadi Ahmadi, Ashish Kisti
 Hajian, Sara
 Hanzlik, Lucjan
 Hedin, Daniel
 Herfert, Michael
 Herrmann, Michael
 Heuser, Stephan
 Hoens, T. Ryan
 Holzer, Andreas
 Hosek, Petr
 Idrees, Sabir
 Jansen, Rob
 Jhawar, Mahavir
 Jia, Limin
 Joaquim, Rui
 Jonker, Hugo

Jorgensen, Zachery
 Joye, Marc
 Kalabis, Lukas
 Kamara, Seny
 Keppler, David
 Khader, Dalia
 Klaedtke, Felix
 Kluczniak, Kamil
 Komanduri, Saranga
 Konidala, Divyan
 Kordy, Barbara
 Kostiainen, Kari
 Krzywiecki, Lukas
 Kubiak, Przemysław
 Kumari, Prachi
 Kywe, Su Mon
 Künnemann, Robert
 Lancrenon, Jean
 Li, Jin
 Li, Yan
 Liu, Jia
 Livraga, Giovanni
 Lochbihler, Andreas
 Loftus, Jake
 Lombardi, Flavio
 Lovat, Enrico
 Ma, Di
 Magazinius, Jonas
 Majcher, Krzysztof
 Malacaria, Pasquale
 Malisa, Luka
 Manulis, Mark
 Marinovic, Srdjan
 Mathur, Suhas
 Maurice, Clementine
 Mazurek, Michelle
 Meadows, Catherine
 Meier, Stefan
 Min, Byungho
 Mitrou, Lilian
 Moataz, Tarik
 Molinaro, Cristian
 Mood, Benjamin
 Moyano, Francisco
 Muehlberg, Jan Tobias

Mutti, Simone
 Mylonas, Alexis
 Netter, Michael
 Nikiforakis, Nick
 Nojoimian, Mehrdad
 Nuñez, David
 Oligeri, Gabriele
 Omote, Kazumasa
 Orlandi, Claudio
 Oswald, Elisabeth
 Oya, Simon
 Palazzi, Bernardo
 Pang, Jun
 Paterson, Maura
 Paul, Giura
 Peacock, Thea
 Peeters, Roel
 Peroli, Michele
 Peters, Thomas
 Petit, Jonathan
 Phillips, Joshua
 Pieczul, Olgierd
 Pinto, Alexandre
 Poettering, Bertram
 Pujol, Marta
 Qin, Zhan
 Radomirovic, Sasa
 Rafnsson, Willard
 Ranganathan, Aanjhan
 Ranise, Silvio
 Reisser, Andreas
 Rial, Alfredo
 Riesner, Moritz
 Rijmen, Vincent
 Riva, Ben
 Roman, Rodrigo
 Saracino, Andrea
 Sayaf, Rula
 Scerri, Guillaume
 Schneider, Thomas
 Schuldt, Jacob
 Schulz, Steffen
 Schunter, Matthias
 Sepehrdad, Pouyan
 Sgandurra, Daniele

Shafiq, Basit
Shakarian, Paulo
Shen, Entong
Shi, Jie
Shirazi, Fatemeh
Shulman, Haya
Simo, Hervais
Smans, Jan
Smith, Geoffrey
Soria Comas, Jordi
Soriente, Claudio
Soupionis, Yannis
Squarcina, Marco
Stebila, Douglas
Stefanov, Emil
Stopczynski, Martin
Struminski, Tomasz
Sun, Wenhai
Syverson, Paul
Tews, Erik
Theoharidou, Marianthi
Torabi Dashti, Mohammad
Toz, Deniz
Tsoumas, Bill
Tuerpe, Sven
Tupakula, Uday

Van Acker, Steven
Verde, Nino Vincenzo
Villani, Antonio
Virvilis, Nick
Vitali, Domenico
Wachsmann, Christian
Wang, Bing
Wang, Lusha
Watson, Gaven J.
Weber, Michael
Wei, Wei
Wüchner, Tobias
Yan, Qiben
Yautsiukhin, Artsiom
Yu, Jiangshan
Zagorski, Filip
Zanella-Béguelin, Santiago
Zhang, Bingsheng
Zhang, Liang Feng
Zhang, Ning
Zhang, Tao
Zhang, Xifan
Zhang, Yihua
Zhou, Lan
Zugenmaier, Alf

Table of Contents

Cryptography and Computation

Practical Covertly Secure MPC for Dishonest Majority – Or: Breaking the SPDZ Limits	1
<i>Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart</i>	
Practical and Employable Protocols for UC-Secure Circuit Evaluation over $\mathbb{Z}_n$	19
<i>Jan Camenisch, Robert R. Enderlein, and Victor Shoup</i>	
Privacy-Preserving Accountable Computation	38
<i>Michael Backes, Dario Fiore, and Esfandiar Mohammadi</i>	

Measurement and Evaluation

Verifying Web Browser Extensions' Compliance with Private-Browsing Mode	57
<i>Benjamin S. Lerner, Liam Elberty, Neal Poole, and Shriram Krishnamurthi</i>	
A Quantitative Evaluation of Privilege Separation in Web Browser Designs	75
<i>Xinshu Dong, Hong Hu, Prateek Saxena, and Zhenkai Liang</i>	
Estimating Asset Sensitivity by Profiling Users	94
<i>Youngja Park, Christopher Gates, and Stephen C. Gates</i>	

Applications of Cryptography

Practical Secure Logging: Seekable Sequential Key Generators	111
<i>Giorgia Azzurra Marson and Bertram Poettering</i>	
Request-Based Comparable Encryption	129
<i>Jun Furukawa</i>	
Ensuring File Authenticity in Private DFA Evaluation on Encrypted Files in the Cloud	147
<i>Lei Wei and Michael K. Reiter</i>	

Code Analysis

HI-CFG: Construction by Binary Analysis and Application to Attack Polymorphism	164
<i>Dan Caselden, Alex Bazhanyuk, Mathias Payer, Stephen McCamant, and Dawn Song</i>	

AnDarwin: Scalable Detection of Semantically Similar Android Applications	182
<i>Jonathan Crussell, Clint Gibler, and Hao Chen</i>	

BISTRO: Binary Component Extraction and Embedding for Software Security Applications	200
<i>Zhui Deng, Xiangyu Zhang, and Dongyan Xu</i>	

Network Security

Vulnerable Delegation of DNS Resolution	219
<i>Amir Herzberg and Haya Shulman</i>	

Formal Approach for Route Agility against Persistent Attackers	237
<i>Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan</i>	

Plug-and-Play IP Security: Anonymity Infrastructure instead of PKI ...	255
<i>Yossi Gilad and Amir Herzberg</i>	

Formal Models and Methods

Managing the Weakest Link: A Game-Theoretic Approach for the Mitigation of Insider Threats	273
<i>Aron Laszka, Benjamin Johnson, Pascal Schöttle, Jens Grossklags, and Rainer Böhme</i>	

Automated Security Proofs for Almost-Universal Hash for MAC Verification	291
<i>Martin Gagné, Pascal Lafourcade, and Yassine Lakhnech</i>	

Bounded Memory Protocols and Progressing Collaborative Systems	309
<i>Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov</i>	

Universally Composable Key-Management	327
<i>Steve Kremer, Robert Künnemann, and Graham Steel</i>	

Protocol Analysis

A Cryptographic Analysis of OPACITY (Extended Abstract)	345
<i>Özgür Dagdelen, Marc Fischlin, Tommaso Gagliardoni, Giorgia Azzurra Marson, Arno Mittelbach, and Cristina Onete</i>	
Symbolic Probabilistic Analysis of Off-Line Guessing	363
<i>Bruno Conchinha, David Basin, and Carlos Caleiro</i>	
ASICS: Authenticated Key Exchange Security Incorporating Certification Systems	381
<i>Colin Boyd, Cas Cremers, Michèle Feltz, Kenneth G. Paterson, Bertram Poettering, and Douglas Stebila</i>	

Privacy Enhancing Models and Technologies

Efficient Privacy-Enhanced Familiarity-Based Recommender System . . .	400
<i>Arjan Jeckmans, Andreas Peter, and Pieter Hartel</i>	
Privacy-Preserving User Data Oriented Services for Groups with Dynamic Participation	418
<i>Dmitry Kononchuk, Zekeriya Erkin, Jan C.A. van der Lubbe, and Reginald L. Lagendijk</i>	
Privacy-Preserving Matching of Community-Contributed Content	443
<i>Mishari Almishari, Paolo Gasti, Gene Tsudik, and Ekin Oguz</i>	

E-voting and Privacy

Ballot Secrecy and Ballot Independence Coincide	463
<i>Ben Smyth and David Bernhard</i>	
Election Verifiability or Ballot Privacy: Do We Need to Choose?	481
<i>Édouard Cuvelier, Olivier Pereira, and Thomas Peters</i>	
Enforcing Privacy in the Presence of Others: Notions, Formalisations and Relations	499
<i>Naipeng Dong, Hugo Jonker, and Jun Pang</i>	

Malware Detection

Mining Malware Specifications through Static Reachability Analysis . . .	517
<i>Hugo Daniel Macedo and Tayssir Touili</i>	
Patrol: Revealing Zero-Day Attack Paths through Network-Wide System Object Dependencies	536
<i>Jun Dai, Xiaoyan Sun, and Peng Liu</i>	

Measuring and Detecting Malware Downloads in Live Network Traffic	556
<i>Phani Vadrevu, Babak Rahbarinia, Roberto Perdisci, Kang Li, and Manos Antonakakis</i>	

Access Control

Automated Certification of Authorisation Policy Resistance	574
<i>Andreas Griesmayer and Charles Morisset</i>	
Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption	592
<i>Jin Li, Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma, and Wenjing Lou</i>	
Purpose Restrictions on Information Use	610
<i>Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing</i>	
Distributed Shuffling for Preserving Access Confidentiality	628
<i>Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Gerardo Pelosi, and Pierangela Samarati</i>	

Attacks

Range Extension Attacks on Contactless Smart Cards	646
<i>Yossef Oren, Dvir Schirman, and Avishai Wool</i>	
CellFlood: Attacking Tor Onion Routers on the Cheap	664
<i>Marco Valerio Barbera, Vasileios P. Kemerlis, Vasilis Pappas, and Angelos D. Keromytis</i>	
Nowhere to Hide: Navigating around Privacy in Online Social Networks	682
<i>Mathias Humbert, Théophile Studer, Matthias Grossglauser, and Jean-Pierre Hubaux</i>	
Current Events: Identifying Webpages by Tapping the Electrical Outlet	700
<i>Shane S. Clark, Hossen Mustafa, Benjamin Ransford, Jacob Sorber, Kevin Fu, and Wenjuan Xu</i>	

Language-Based Protection

Eliminating Cache-Based Timing Attacks with Instruction-Based Scheduling	718
<i>Deian Stefan, Pablo Buiras, Edward Z. Yang, Amit Levy, David Terei, Alejandro Russo, and David Mazières</i>	

Data-Confined HTML5 Applications	736
<i>Devdatta Akhawe, Frank Li, Warren He, Prateek Saxena, and Dawn Song</i>	
KQguard: Binary-Centric Defense against Kernel Queue Injection Attacks	755
<i>Jinpeng Wei, Feng Zhu, and Calton Pu</i>	
Run-Time Enforcement of Information-Flow Properties on Android (Extended Abstract)	775
<i>Limin Jia, Jassim Aljuraidean, Elli Fragkaki, Lujo Bauer, Michael Stroucken, Kazuhide Fukushima, Shinsaku Kiyomoto, and Yutaka Miyake</i>	
Author Index	793