

2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2018)

**London, United Kingdom
23-27 April 2018**



**IEEE Catalog Number: CFP18N35-POD
ISBN: 978-1-5386-5446-0**

**Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP18N35-POD
ISBN (Print-On-Demand):	978-1-5386-5446-0
ISBN (Online):	978-1-5386-5445-3

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2018 IEEE European Symposium on Security and Privacy Workshops **EuroSPW 2018**

Table of Contents

Message from the Program and General Chairs .viii.....
Message from the Workshop Chairs .x.....
Organizing Committee .xi.....

SPIDA – Workshop on Security Protocol Implementations: Development and Analysis

Vulnerability Detection on Mobile Applications Using State Machine Inference .1.....
*Wesley van der Lee (Delft University of Technology) and Sicco Verwer
(Delft University of Technology)*

Inferring OpenVPN State Machines Using Protocol State Fuzzing .11.....
*Lesly-Ann Daniel (University of Rennes 1 - ENS Rennes), Erik Poll
(Radboud University), and Joeri de Ruiter (Radboud University)*

EuroUSEC – European Workshop on Usable Security

S&B – Security on Blockchains

Authenticated Data Structures for Privacy-Preserving Monero Light Clients .20.....
*Kevin Lee (University of Illinois at Urbana-Champaign) and Andrew
Miller (University of Illinois at Urbana-Champaign)*

Incentivized Delivery Network of IoT Software Updates Based on Trustless
Proof-of-Distribution .29.....
*Oded Leiba (Ben-Gurion University), Yechiav Yitzchak (Ben-Gurion
University), Ron Bitton (Ben-Gurion University), Asaf Nadler
(Ben-Gurion University), and Asaf Shabtai (Ben-Gurion University)*

How to Squeeze a Crowd: Reducing Bandwidth in Mixing Cryptocurrencies .40.....
*Alishah Chator (Johns Hopkins University) and Matthew Green (Johns
Hopkins University)*

The Impact of Uncle Rewards on Selfish Mining in Ethereum .50.....
*Fabian Ritz (Munich University of Applied Sciences) and Alf Zugenmaier
(Munich University of Applied Sciences)*

A First Look at Browser-Based Cryptojacking .58.....	
	<i>Shayan Eskandari (Concordia University), Andreas Leoutsarakos (Concordia University), Troy Mursch (Bad Packets Report), and Jeremy Clark (Concordia University)</i>
Blockchain as a Service (BaaS): Providers and Trust .67.....	
	<i>Jatinder Singh (University of Cambridge) and Johan David Michels (Queen Mary University of London)</i>
Decentralizing Digital Identity: Open Challenges for Distributed Ledgers .75.....	
	<i>Paul Dunphy (Innovation Center), Luke Garratt (Innovation Center), and Fabien Petitcolas (Innovation Center)</i>

S4CIP – 3rd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection

IWPE – International Workshop on Privacy Engineering

Interaction-Based Privacy Threat Elicitation .79.....	
	<i>Laurens Sion (KU Leuven), Kim Wuyts (KU Leuven), Koen Yskout (KU Leuven), Dimitri Van Landuyt (KU Leuven), and Wouter Joosen (KU Leuven)</i>
The Odyssey: Modeling Privacy Threats in a Brave New World .87.....	
	<i>Rafa Galvez (imec-COSIC KU Leuven) and Seda Gurses (imec-COSIC KU Leuven)</i>
Privacy Risk Analysis to Enable Informed Privacy Settings .95.....	
	<i>Sourya Joyee De (Inria) and Daniel Le Metayer (Inria)</i>
FP -TESTER : Automated Testing of Browser Fingerprint Resilience .103.....	
	<i>Antoine Vastel (University of Lille / INRIA), Walter Rudametkin (University of Lille / INRIA), and Romain Rouvoy (University of Lille / INRIA / IUF)</i>
Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering .108....	
	<i>Yod-Samuel Martin (Universidad Politecnica de Madrid) and Antonio Kung (Trialog)</i>
It Takes a Village: A Community Based Participatory Framework for Privacy Design .112.....	
	<i>Darakshhan J. Mir (Bucknell University), Yan Shvartzshnaider (New York University), and Mark Latonero (Data and Society Research Institution)</i>
Enhancing Transparency and Consent in the IoT .116.....	
	<i>Claude Castelluccia (Inria), Mathieu Cunche (INSA de Lyon), Daniel Le Metayer (Inria), and Victor Morel (Inria)</i>
Privacy Compliance Via Model Transformations .120.....	
	<i>Thibaud Antignac (French Atomic Energy Commission), Riccardo Scandariato (University of Gothenburg), and Gerardo Schneider (University of Gothenburg)</i>
Simulation of a Trust and Reputation Based Mitigation Protocol for a Black Hole Style Attack on VANETs .127.....	
	<i>Giuseppe Primiero (Middlesex University London), Agostino Martorana (Middlesex University London), and Jacopo Tagliabue (Tooso Inc.)</i>

Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability .136.....
Andrea Hoeller (Infineon Technologies Austria AG) and Ronald Toegl (Infineon Technologies Austria AG)

The Secret Processor Will Go to the Ball: Benchmark Insider-Proof Encrypted Computing .145.....
Peter T. Breuer (Hecusys LLC), Jonathan P. Bowen (London South Bank University), Esther Palomar (Birmingham City University), and Zhiming Liu (Southwest University)

An Analysis of Cyber Security Attack Taxonomies .153.....
Richard Derbyshire (Lancaster University), Benjamin Green (Lancaster University), Daniel Prince (Lancaster University), Andreas Mauthe (Lancaster University), and David Hutchison (Lancaster University)

Author Index .163