

2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2017)

**Paris, France
29 – 30 April 2017**



**IEEE Catalog Number: CFP17N35-POD
ISBN: 978-1-5386-2245-2**

**Copyright © 2017 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:	CFP17N35-POD
ISBN (Print-On-Demand):	978-1-5386-2245-2
ISBN (Online):	978-1-5386-2244-5

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

2017 IEEE European Symposium on Security and Privacy Workshops

EuroSPW 2017

Table of Contents

Message from the EuroSP 2017 General Chair.....	viii
Organizing Committee.....	xi
Workshop Committees.....	xiii

IEEE Security and Privacy on the Blockchain (S&B) Workshop

Introduction to Security and Privacy on the Blockchain	1
<i>Harry Halpin and Marta Piekarska</i>	
Zero-Collateral Lotteries in Bitcoin and Ethereum	4
<i>Andrew Miller and Iddo Bentov</i>	
Design of a Privacy-Preserving Decentralized File Storage with Financial Incentives	14
<i>Henning Kopp, David Mödinger, Franz Hauck, Frank Kargl, and Christoph Bösch</i>	
Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies	23
<i>Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford</i>	
BIP32-Ed25519: Hierarchical Deterministic Keys over a Non-linear Keyspace	27
<i>Dmitry Khovratovich and Jason Law</i>	
Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques	32
<i>Malte Möser and Rainer Böhme</i>	
Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography	42
<i>Masashi Sato and Shin'ichi Matsuo</i>	
Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain	50
<i>Aymen Boudguiga, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau, Flavien Quesnel, Anthony Roger, and Renaud Sirdey</i>	
Auditable Zerocoin	59
<i>Ken Naganuma, Masayuki Yoshino, Hisayoshi Sato, and Takayuki Suzuki</i>	

Conditions of Full Disclosure: The Blockchain Remuneration Model	64
<i>S. Matthew English and Ehsan Nezhadian</i>	
Oligarchic Control of Business-to-Business Blockchains	68
<i>Leif-Nissen Lundbaek and Michael Huth</i>	

IMPS 2017: Innovations in Mobile Privacy & Security Workshop

The Privacy API: Facilitating Insights in How One's Own User Data is Shared	72
<i>Bram Bonné, Peter Quax, and Wim Lamotte</i>	
The Cost of Push Notifications for Smartphones Using Tor Hidden Services	76
<i>Stephan A. Kollmann and Alastair R. Beresford</i>	

SEMS: Workshop on Security for Embedded and Mobile Systems

Secure and Efficient RNS Software Implementation for Elliptic Curve Cryptography	86
<i>Apostolos P. Fournaris, Louiza Papachristodoulou, and Nicolas Sklavos</i>	
From Smashed Screens to Smashed Stacks: Attacking Mobile Phones Using Malicious Aftermarket Parts	94
<i>Omer Shwartz, Guy Shitrit, Asaf Shabtai, and Yossi Oren</i>	
The Curious Case of the Curious Case: Detecting Touchscreen Events Using a Smartphone Protective Case	99
<i>Tomer Gluck, Rami Puzis, Yossi Oren, and Asaf Shabtai</i>	
Use of Simulators for Side-Channel Analysis	104
<i>Nikita Veshchikov and Sylvain Guilley</i>	
Practical Power Analysis on KCipher-2 Software on Low-End Microcontrollers	113
<i>Wataru Kawai, Rei Ueno, Naofumi Homma, Takafumi Aoki, Kazuhide Fukushima, and Shinsaku Kiyomoto</i>	
Are You Really My Friend? Efficient and Secure Friend-Matching in Mobile Social Networks	122
<i>Mohammad Etemad, Filipe Beato, Alptekin Küpçü, and Bart Preneel</i>	

S4CIP'17: 2nd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection

Cyber-Attack Detection for Industrial Control System Monitoring with Support Vector Machine Based on Communication Profile	132
<i>Asuka Terai, Shingo Abe, Shoya Kojima, Yuta Takano, and Ichiro Koshijima</i>	
Challenges and Approaches in Securing Safety-Relevant Railway Signalling	139
<i>Christian Schlehuber, Markus Heinrich, Tsvetoslava Vateva-Gurova, Stefan Katzenbeisser, and Neeraj Suri</i>	
A Proof-Theoretic Trust and Reputation Model for VANET	146
<i>Giuseppe Primiero, Franco Raimondi, Taolue Chen, and Rajagopal Nagarajan</i>	
Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems	153
<i>Zhendong Ma, Aleksandar Hudic, Abdelkader Shaaban, and Sandor Plosz</i>	

Using Process Mining and Model-Driven Engineering to Enhance Security of Web Information Systems	160
<i>Simona Bernardi, Raúl Piracés Alastuey, and Raquel Trillo-Lado</i>	
Towards a Unified Definition of Cyber and Physical Vulnerability in Critical Infrastructures	167
<i>Stefano Marrone</i>	
Formal Analysis of Safety and Security Requirements of Critical Systems Supported by an Extended STPA Methodology	174
<i>Giles Howard, Michael Butler, John Colley, and Vladimiro Sassone</i>	
Author Index	181