

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

**London, United Kingdom
24-26 April 2018**



**IEEE Catalog Number: CFP18C75-POD
ISBN: 978-1-5386-4229-0**

**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:	CFP18C75-POD
ISBN (Print-On-Demand):	978-1-5386-4229-0
ISBN (Online):	978-1-5386-4228-3

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 **EuroSP 2018**

Table of Contents

Message from the Chairs	x
Organizing Committee	xii
Steering Committee	xiii
Program Committee	xiv

Language-Based Security and Access Control

What You Get is What You C: Controlling Side Effects in Mainstream C Compilers	1
<i>Laurent Simon (University of Cambridge), David Chisnall (University of Cambridge), and Ross Anderson (University of Cambridge)</i>	
COVERN: A Logic for Compositional Verification of Information Flow Control	16
<i>Toby Murray (University of Melbourne and Data61), Robert Sison (UNSW and Data61), and Kai Engelhardt (UNSW and Data61)</i>	
Mining ABAC Rules from Sparse Logs	31
<i>Carlos Cotrini (ETH Zürich), Thilo Weghorn (ETH Zürich), and David Basin (ETH Zürich)</i>	

Security and Privacy Analysis

I Spy with My Little Eye: Analysis and Detection of Spying Browser Extensions	47
<i>Anupama Aggarwal (IIIT-Delhi), Bimal Viswanath (UC Santa Barbara), Liang Zhang (Northeastern University), Saravana Kumar (CEG), Ayush Shah (IIIT-Delhi), and Ponnurangam Kumaraguru (IIIT-Delhi)</i>	
Dissecting Privacy Risks in Biomedical Data	62
<i>Pascal Berrang (CISPA), Mathias Humbert (Swiss Data Science Center), Yang Zhang (CISPA), Irina Lehmann (Helmholtz Center for Environmental Research Leipzig), Roland Eils (German Cancer Research Center (DKFZ) and University of Heidelberg), and Michael Backes (CISPA Helmholtz Center i.G.)</i>	
Formally Reasoning about the Cost and Efficacy of Securing the Email Infrastructure	77
<i>Patrick Speicher (CISPA), Marcel Steinmetz (CISPA), Robert Künnemann (CISPA), Milivoj Simeonovski (CISPA), Giancarlo Pellegrino (CISPA), Jörg Hoffmann (CISPA), and Michael Backes (CISPA Helmholtz Center i.G.)</i>	

Network and Communication Security

Language-Independent Synthesis of Firewall Policies .92.....	
<i>Chiara Bodei (Dipartimento di Informatica), Pierpaolo Degano (Dipartimento di Informatica), Letterio Galletta (Dipartimento di Informatica), Riccardo Focardi (DAIS), Mauro Tempesta (DAIS), and Lorenzo Veronese (DAIS)</i>	
The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication .107.....	
<i>Martin Strohmeier (University of Oxford), Matthew Smith (University of Oxford), Vincent Lenders (armasuisse), and Ivan Martinovic (University of Oxford)</i>	
Masters of Time: An Overview of the NTP Ecosystem .122.....	
<i>Teemu Ryttilahti (Ruhr-University Bochum), Dennis Tatang (Ruhr-University Bochum), Janosch Köpper (Ruhr-University Bochum), and Thorsten Holz (Ruhr-University Bochum)</i>	
TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer .137.....	
<i>Chen Chen (Carnegie Mellon University), Daniele E. Asoni (ETH Zürich), Adrian Perrig (ETH Zürich), David Barrera (Polytechnique Montreal), George Danezis (University College London), and Carmela Troncoso (EPFL)</i>	

System Security

Eraser: Your Data Won't Be Back .153.....	
<i>Kaan Onarlioglu (Akamai Technologies), William Robertson (Northeastern University), and Engin Kirda (Northeastern University)</i>	
Security Risks in Asynchronous Web Servers: When Performance Optimizations Amplify the Impact of Data-Oriented Attacks .167.....	
<i>Micah Morton (University of North Carolina at Chapel Hill), Jan Werner (University of North Carolina at Chapel Hill), Panagiotis Kintis (Georgia Institute of Technology), Kevin Snow (Zeropoint Dynamics), Manos Antonakakis (Georgia Institute of Technology), Michalis Polychronakis (Stony Brook University), and Fabian Monroe (University of North Carolina at Chapel Hill)</i>	
Have Your PI and Eat it Too: Practical Security on a Low-Cost Ubiquitous Computing Platform .183.....	
<i>Amit Vasudevan (SEI) and Sagar Chaki (SEI)</i>	
Get in Line: Ongoing Co-presence Verification of a Vehicle Formation Based on Driving Trajectories .199.....	
<i>Christian Vaas (University of Oxford), Mika Juuti (Aalto University), N. Asokan (Aalto University), and Ivan Martinovic (University of Oxford)</i>	

Software Security

- Sponge-Based Control-Flow Protection for IoT Devices .214.....
Mario Werner (Graz University of Technology), Thomas Unterluggauer (Graz University of Technology), David Schaffenrath (Graz University of Technology), and Stefan Mangard (Graz University of Technology)
- Position-Independent Code Reuse: On the Effectiveness of ASLR in the Absence of Information Disclosure .227.....
Enes Göktas (Vrije Universiteit Amsterdam), Benjamin Kollenda (Ruhr-University Bochum, Germany), Philipp Koppe (Ruhr-University Bochum, Germany), Erik Bosman (Vrije Universiteit Amsterdam), Georgios Portokalidis (Stevens Institute of Technology), Thorsten Holz (Ruhr-University Bochum, Germany), Herbert Bos (Vrije Universiteit Amsterdam), and Cristiano Giuffrida (Vrije Universiteit Amsterdam)
- Probabilistic Obfuscation Through Covert Channels .243.....
Jon Stephens (The University of Arizona), Babak Yadegari (The University of Arizona), Christian Collberg (The University of Arizona), Saumya Debray (The University of Arizona), and Carlos Scheidegger (The University of Arizona)

Applied Cryptography 1

- Understanding User Tradeoffs for Search in Encrypted Communication .258.....
Wei Bai (University of Maryland), Ciara Lynton (University of Maryland), Charalampos Papamanthou (University of Maryland), and Michelle L. Mazurek (University of Maryland)
- Short Double- and N-Times-Authentication-Preventing Signatures from ECDSA and More .273.....
David Derler (IAIK), Sebastian Ramacher (IAIK), and Daniel Slamanig (AIT Austrian Institute of Technology)
- Crypto Crumple Zones: Enabling Limited Access without Mass Surveillance .288.....
Charles Wright (Portland State University) and Mayank Varia (Boston University)

Session Side Channels and Fault Attacks

- Online Synthesis of Adaptive Side-Channel Attacks Based On Noisy Observations .307.....
Lucas Bang (University of California Santa Barbara), Nicolas Rosner (University of California Santa Barbara), and Tevfik Bultan (University of California Santa Barbara)
- User Blocking Considered Harmful? An Attacker-Controllable Side Channel to Identify Social Accounts .323.....
Takuya Watanabe (NTT Secure Platform Laboratories), Eitaro Shioji (NTT Secure Platform Laboratories), Mitsuaki Akiyama (NTT Secure Platform Laboratories), Keito Sasaoka (NTT Secure Platform Laboratories), Takeshi Yagi (NTT Secure Platform Laboratories), and Tatsuya Mori (NTT Secure Platform Laboratories)

Attacking Deterministic Signature Schemes Using Fault Attacks .338.....	
<i>Damian Poddebniak (Munster University of Applied Sciences), Juraj Somorovsky (Ruhr University Bochum), Sebastian Schinzel (Munster University of Applied Sciences), Manfred Lochter (Federal Office for Information Security), and Paul Rösler (Ruhr University Bochum)</i>	

Applied Cryptography 2

CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM .353.....	
<i>Joppe Bos (NXP Semiconductors), Leo Ducas (CWI Amsterdam), Eike Kiltz (Ruhr-University Bochum), T Lepoint (SRI International), Vadim Lyubashevsky (IBM Research Zurich), John M. Schanck (University of Waterloo), Peter Schwabe (Radboud University), Gregor Seiler (IBM Research Zurich), and Damien Stehle (ENS de Lyon)</i>	
Just In Time Hashing .368.....	
<i>Benjamin Harsha (Purdue University) and Jeremiah Blocki (Purdue University)</i>	
In Search of CurveSwap: Measuring Elliptic Curve Implementations in the Wild .384.....	
<i>Luke Valenta (University of Pennsylvania), Nick Sullivan (Cloudflare), Antonio Sanso (Adobe), and Nadia Heninger (University of Pennsylvania)</i>	

Systematization of Knowledge

SoK: Security and Privacy in Machine Learning .399.....	
<i>Nicolas Papernot (Pennsylvania State University), Patrick McDaniel (Pennsylvania State University), Arunesh Sinha (University of Michigan), and Michael P. Wellman (University of Michigan)</i>	

Protocol Security

More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema .415...	
<i>Paul Rösler (Ruhr-University Bochum), Christian Mainka (Ruhr-University Bochum), and Jörg Schwenk (Ruhr-University Bochum)</i>	
A Formal Analysis of the Neuchatel e-Voting Protocol .430.....	
<i>Veronique Cortier (CNRS), David Galindo (University of Birmingham), and Mathieu Turuani (INRIA)</i>	
On Composability of Game-Based Password Authenticated Key Exchange .443.....	
<i>Marjan Skrobot (University of Luxembourg) and Jean Lancrenon (itrust consulting)</i>	

Security and Learning

ChainSmith: Automatically Learning the Semantics of Malicious Campaigns by Mining Threat Intelligence Reports .458.....	
<i>Ziyun Zhu (University of Maryland) and Tudor Dumitras (University of Maryland)</i>	

DeepRefiner: Multi-layer Android Malware Detection System Applying Deep Neural Networks .473...	
<i>Ke Xu (Singapore Management University), Yingjiu Li (Singapore Management University), Robert H. Deng (Singapore Management University), and Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences)</i>	
Forgotten Siblings: Unifying Attacks on Machine Learning and Digital Watermarking .488.....	
<i>Erwin Quiring (TU Braunschweig), Daniel Arp (TU Braunschweig), and Konrad Rieck (TU Braunschweig)</i>	
Author Index 503	