

# **2019 IEEE Symposium on Security and Privacy (SP 2019)**

**San Francisco, California, USA  
19 – 23 May 2019**

**Pages 1-723**



**IEEE Catalog Number: CFP19020-POD  
ISBN: 978-1-5386-6661-6**

**Copyright © 2019 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:	CFP19020-POD
ISBN (Print-On-Demand):	978-1-5386-6661-6
ISBN (Online):	978-1-5386-6660-9
ISSN:	1081-6011

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2019 IEEE Symposium on Security and Privacy **SP 2019**

## Table of Contents

Message from the General Chair .....	xvi
Message from the Program Chairs .....	xix
Organizing Committee .....	xx
Program Committee .....	xxii

### Session 1: Hardware Security

Spectre Attacks: Exploiting Speculative Execution .....	1
<i>Paul Kocher (Independent (www.paulkocher.com)), Jann Horn (Google Project Zero), Anders Fogh (G DATA Advanced Analytics), Daniel Genkin (University of Pennsylvania and University of Maryland), Daniel Gruss (Graz University of Technology), Werner Haas (Cyberus Technology), Mike Hamburg (Rambus, Cryptography Research Division), Moritz Lipp (Graz University of Technology), Stefan Mangard (Graz University of Technology), Thomas Prescher (Cyberus Technology), Michael Schwarz (Graz University of Technology), and Yuval Yarom (University of Adelaide and Data61)</i>	
SoK: The Challenges, Pitfalls, and Perils of Using Hardware Performance Counters for Security .....	20
<i>Sanjeev Das (University of North Carolina at Chapel Hill), Jan Werner (University of North Carolina at Chapel Hill), Manos Antonakakis (Georgia Institute of Technology), Michalis Polychronakis (Stony Brook University), and Fabian Monrose (University of North Carolina at Chapel Hill)</i>	
Theory and Practice of Finding Eviction Sets .....	39
<i>Pepe Vila (IMDEA Software Institute/Technical University of Madrid (UPM)), Boris Köpf (Microsoft Research), and José F. Morales (IMDEA Software Institute)</i>	
Exploiting Correcting Codes: On the Effectiveness of ECC Memory Against Rowhammer Attacks .....	55
<i>Lucian Cojocar (Vrije Universiteit Amsterdam), Kaveh Razavi (Vrije Universiteit Amsterdam), Cristiano Giuffrida (Vrije Universiteit Amsterdam), and Herbert Bos (Vrije Universiteit Amsterdam)</i>	
Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives .....	72
<i>Carlo Meijer (Radboud University) and Bernard van Gastel (Open University of the Netherlands / Radboud University)</i>	

RIDL: Rogue In-Flight Data Load .....	88
<i>Stephan van Schaik (Vrije Universiteit Amsterdam), Alyssa Milburn (Vrije Universiteit Amsterdam), Sebastian Österlund (Vrije Universiteit Amsterdam), Pietro Frigo (Vrije Universiteit Amsterdam), Giorgi Maisuradze (CISPA Helmholtz Center for Information Security), Kaveh Razavi (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam), and Cristiano Giuffrida (Vrije Universiteit Amsterdam)</i>	

## Session 2: Blockchain & Cryptocurrency

Perun: Virtual Payment Hubs over Cryptocurrencies .....	106
<i>Stefan Dziembowski (University of Warsaw), Lisa Eckey (TU Darmstadt), Sebastian Faust (TU Darmstadt), and Daniel Malinowski (University of Warsaw)</i>	
Redactable Blockchain in the Permissionless Setting .....	124
<i>Dominic Deuber (Friedrich-Alexander-University Erlangen-Nurnberg), Bernardo Magri (Aarhus University), and Sri Aravinda Krishnan Thyagarajan (Friedrich-Alexander-University Erlangen-Nurnberg)</i>	
Proof-of-Stake Sidechains .....	139
<i>Peter Gaži (IOHK), Aggelos Kiayias (University of Edinburgh, IOHK), and Dionysis Zindros (University of Athens, IOHK)</i>	
Ouroboros Crispinus: Privacy-Preserving Proof-of-Stake .....	157
<i>Thomas Kerber (The University of Edinburgh &amp; IOHK), Aggelos Kiayias (The University of Edinburgh &amp; IOHK), Markulf Kohlweiss (The University of Edinburgh &amp; IOHK), and Vassilis Zikas (The University of Edinburgh &amp; IOHK)</i>	
Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security .....	175
<i>Ren Zhang (Nervos and imec-COSIC, KU Leuven) and Bart Preneel (imec-COSIC, KU Leuven)</i>	
XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets .....	193
<i>Alexei Zamyatin (Imperial College London &amp; SBA Research), Dominik Harz (Imperial College London), Joshua Lind (Imperial College London), Panayiotis Panayiotou (Imperial College London), Arthur Gervais (Imperial College London), and William Knottenbelt (Imperial College London)</i>	

## Session 3: Web Security

Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate .....	211
<i>Emily Stark (Google), Ryan Sleevi (Google), Rijad Muminovic (University of Sarajevo), Devon O'Brien (Google), Eran Messeri (Google), Adrienne Porter Felt (Google), Brendan McMillion (Cloudflare), and Parisa Tabriz (Google)</i>	
EmPoWeb: Empowering Web Applications with Browser Extensions .....	227
<i>Dolière Francis Somé (Université Côte d'Azur/Inria, France)</i>	

"If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS .....	246
<i>Katharina Krombholz (CISPA Helmholtz Center for Information Security), Karoline Busse (Bonn University), Katharina Pfeffer (SBA Research), Matthew Smith (Bonn University / FhG FKIE), and Emanuel von Zezschwitz (Bonn University / FhG FKIE)</i>	
FideliuS: Protecting User Secrets from Compromised Browsers .....	264
<i>Saba Eskandarian (Stanford University), Jonathan Cogan (Stanford University), Sawyer Birnbaum (Stanford University), Peh Chang Wei Brandon (Stanford University), Dillon Franke (Stanford University), Forest Fraser (Stanford University), Gaspar Garcia (Stanford University), Eric Gong (Stanford University), Hung T. Nguyen (Stanford University), Tareh K. Sethi (Stanford University), Vishal Subbiah (Stanford University), Michael Backes (CISPA Helmholtz Center for Information Security), Giancarlo Pellegrino (Stanford University/CISPA Helmholtz Center for Information Security), and Dan Boneh (Stanford University)</i>	
Postcards from the Post-HTTP World: Amplification of HTTPS Vulnerabilities in the Web Ecosystem .....	281
<i>Stefano Calzavara (Università Ca' Foscari), Riccardo Focardi (Università Ca' Foscari, Cryptosense), Matus Nemeč (Università Ca' Foscari, Masaryk University), Alvis Rabitti (Università Ca' Foscari), and Marco Squarcina (TU Wien)</i>	

## Session 4: Privacy

Towards Practical Differentially Private Convex Optimization .....	299
<i>Roger Iyengar (Carnegie Mellon University), Joseph P. Near (University of California, Berkeley), Dawn Song (University of California, Berkeley), Om Thakkar (Boston University), Abhradeep Thakurta (University of California, Santa Cruz), and Lun Wang (Peking University)</i>	
PrivKV: Key-Value Data Collection with Local Differential Privacy .....	317
<i>Qingqing Ye (Renmin University of China), Haibo Hu (Hong Kong Polytechnic University), Xiaofeng Meng (Renmin University of China), and Huadi Zheng (Hong Kong Polytechnic University)</i>	
Differentially Private Model Publishing for Deep Learning .....	332
<i>Lei Yu (Georgia Institute of Technology), Ling Liu (Georgia Institute of Technology), Calton Pu (Georgia Institute of Technology), Mehmet Emre Gursoy (Georgia Institute of Technology), and Stacey Truex (Georgia Institute of Technology)</i>	
KHyperLogLog: Estimating Reidentifiability and Joinability of Large Data at Scale .....	350
<i>Pern Hui Chia (Google), Damien Desfontaines (ETH Zurich / Google), Irippuge Milinda Perera (Google), Daniel Simmons-Marengo (Google), Chao Li (Google), Wei-Yen Day (Google), Qiushi Wang (Google), and Miguel Guevara (Google)</i>	
Characterizing Pixel Tracking through the Lens of Disposable Email Services .....	365
<i>Hang Hu (Virginia Tech), Peng Peng (Virginia Tech), and Gang Wang (Virginia Tech)</i>	

## Session 6: Protocols and Authentication

Reasoning Analytically about Password-Cracking Software .....	380
<i>Enze Liu (University of Chicago), Amanda Nakanishi (University of Chicago), Maximilian Golla (Ruhr University Bochum), David Cash (University of Chicago), and Blase Ur (University of Chicago)</i>	
True2F: Backdoor-Resistant Authentication Tokens .....	398
<i>Emma Dauterman (Stanford and Google), Henry Corrigan-Gibbs (Stanford), David Mazières (Stanford), Dan Boneh (Stanford), and Dominic Rizzo (Google)</i>	
Beyond Credential Stuffing: Password Similarity Models Using Neural Networks .....	417
<i>Bijeeta Pal (Cornell Tech), Tal Daniel (Technion), Rahul Chatterjee (Cornell Tech), and Thomas Ristenpart (Cornell Tech)</i>	
The 9 Lives of Bleichenbacher's CAT: New Cache ATtacks on TLS Implementations .....	435
<i>Eyal Ronen (Tel Aviv University), Robert Gillham (University of Adelaide), Daniel Genkin (University of Michigan), Adi Shamir (Weizmann Institute), David Wong (NCC Group), and Yuval Yarom (University of Adelaide / Data61)</i>	
An Extensive Formal Security Analysis of the OpenID Financial-Grade API .....	453
<i>Daniel Fett (yes.com AG), Pedram Hosseini (University of Stuttgart), and Ralf Küsters (University of Stuttgart)</i>	

## Session 5: Program Analysis

Asm2Vec: Boosting Static Representation Robustness for Binary Clone Search against Code Obfuscation and Compiler Optimization .....	472
<i>Steven H. H. Ding (McGill University), Benjamin C. M. Fung (McGill University), and Philippe Charland (Defence R&amp;D Canada - Valcartier, Canada)</i>	
Iodine: Fast Dynamic Taint Tracking Using Rollback-free Optimistic Hybrid Analysis .....	490
<i>Subarno Banerjee (University of Michigan), David Devecsery (Georgia Institute of Technology), Peter M. Chen (University of Michigan), and Satish Narayanasamy (University of Michigan)</i>	
CaSym: Cache Aware Symbolic Execution for Side Channel Detection and Mitigation .....	505
<i>Robert Brotzman (Pennsylvania State University), Shen Liu (Pennsylvania State University), Danfeng Zhang (Pennsylvania State University), Gang Tan (Pennsylvania State University), and Mahmut Kandemir (Pennsylvania State University)</i>	
Towards Automated Safety Vetting of PLC Code in Real-World Plants .....	522
<i>Mu Zhang (Cornell University), Chien-Ying Chen (University of Illinois at Urbana-Champaign), Bin-Chou Kao (University of Illinois at Urbana-Champaign), Yassine Qamsane (University of Michigan), Yuru Shao (University of Michigan), Yikai Lin (University of Michigan), Elaine Shi (Cornell University), Sibin Mohan (University of Illinois at Urbana-Champaign), Kira Barton (University of Michigan), James Moyne (University of Michigan), and Z. Morley Mao (University of Michigan)</i>	

Using Safety Properties to Generate Vulnerability Patches .....	539
<i>Zhen Huang (Pennsylvania State University and University of Toronto), David Lie (University of Toronto), Gang Tan (Pennsylvania State University), and Trent Jaeger (Pennsylvania State University)</i>	

## Session 7: Mobile and Location Security

Short Text, Large Effect: Measuring the Impact of User Reviews on Android App Security & Privacy .....	555
<i>Duc Cuong Nguyen (CISPA, Saarland University), Erik Derr (CISPA, Saarland University), Michael Backes (CISPA Helmholtz Center i.G.), and Sven Bugiel (CISPA Helmholtz Center i.G.)</i>	
Demystifying Hidden Privacy Settings in Mobile Apps .....	570
<i>Yi Chen (Indiana University Bloomington, University of Chinese Academy of Sciences), Mingming Zha (Institute of Information Engineering, Chinese Academy of Sciences), Nan Zhang (Indiana University Bloomington), Dandan Xu (Institute of Information Engineering, Chinese Academy of Sciences), Qianqian Zhao (Institute of Information Engineering, Chinese Academy of Sciences), Xuan Feng (Institute of Information Engineering, Chinese Academy of Sciences), Kan Yuan (Indiana University Bloomington), Fnu Suya (The University of Virginia), Yuan Tian (The University of Virginia), Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences), XiaoFeng Wang (Indiana University Bloomington), and Wei Zou (Institute of Information Engineering, Chinese Academy of Sciences)</i>	
Security of GPS/INS Based On-road Location Tracking Systems .....	587
<i>Sashank Narain (Northeastern University), Aanjan Ranganathan (Northeastern University), and Guevara Noubir (Northeastern University)</i>	
Understanding the Security of ARM Debugging Features .....	602
<i>Zhenyu Ning (Wayne State University) and Fengwei Zhang (Wayne State University)</i>	
Tap 'n Ghost: A Compilation of Novel Attack Techniques against Smartphone Touchscreens .....	620
<i>Seita Maruyama (Waseda University), Satohiro Wakabayashi (Waseda University), and Tatsuya Mori (Waseda University / RIKEN AIP)</i>	
SensorID: Sensor Calibration Fingerprinting for Smartphones .....	638
<i>Jiexin Zhang (University of Cambridge), Alastair R. Beresford (University of Cambridge), and Ian Sheret (Polymath Insight Limited)</i>	

## Session 8: Machine Learning

Certified Robustness to Adversarial Examples with Differential Privacy .....	656
<i>Mathias Lecuyer (Columbia University), Vaggelis Atlidakis (Columbia University), Roxana Geambasu (Columbia University), Daniel Hsu (Columbia University), and Suman Jana (Columbia University)</i>	

DEEPSEC: A Uniform Platform for Security Analysis of Deep Learning Model .....	673
<i>Xiang Ling (Zhejiang University), Shouling Ji (Zhejiang University, Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies), Jiayu Zou (Zhejiang University), Jiannan Wang (Zhejiang University), Chunming Wu (Zhejiang University), Bo Li (UIUC), and Ting Wang (Lehigh University)</i>	
Exploiting Unintended Feature Leakage in Collaborative Learning .....	691
<i>Luca Melis (University College London), Congzheng Song (Cornell University), Emiliano De Cristofaro (University College London), and Vitaly Shmatikov (Cornell Tech)</i>	
Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks .....	707
<i>Bolun Wang (UC Santa Barbara), Yuanshun Yao (University of Chicago), Shawn Shan (University of Chicago), Huiying Li (University of Chicago), Bimal Viswanath (Virginia Tech), Haitao Zheng (University of Chicago), and Ben Y. Zhao (University of Chicago)</i>	
Helen: Maliciously Secure Cooperative Learning for Linear Models .....	724
<i>Wenting Zheng (UC Berkeley), Raluca Ada Popa (UC Berkeley), Joseph E. Gonzalez (UC Berkeley), and Ion Stoica (UC Berkeley)</i>	
Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning .....	739
<i>Milad Nasr (University of Massachusetts Amherst), Reza Shokri (National University of Singapore), and Amir Houmansadr (University of Massachusetts Amherst)</i>	

## Session 9: Fuzzing

Ruzzer: Finding Kernel Race Bugs through Fuzzing .....	754
<i>Dae R. Jeong (KAIST), Kyungtae Kim (Purdue University), Basavesh Shivakumar (Purdue University), Byoungyoung Lee (Seoul National University, Purdue University), and Insik Shin (KAIST)</i>	
ProFuzzer: On-the-fly Input Type Probing for Better Zero-Day Vulnerability Discovery .....	769
<i>Wei You (Purdue University), Xueqiang Wang (Indiana University Bloomington), Shiqing Ma (Purdue University), Jianjun Huang (Renmin University of China), Xiangyu Zhang (Purdue University), XiaoFeng Wang (Indiana University Bloomington), and Bin Liang (Renmin University of China)</i>	
Full-Speed Fuzzing: Reducing Fuzzing Overhead through Coverage-Guided Tracing .....	787
<i>Stefan Nagy (Virginia Tech) and Matthew Hicks (Virginia Tech)</i>	
NEUZZ: Efficient Fuzzing with Neural Program Smoothing .....	803
<i>Dongdong She (Columbia University), Kexin Pei (Columbia University), Dave Epstein (Columbia University), Junfeng Yang (Columbia University), Baishakhi Ray (Columbia University), and Suman Jana (Columbia University)</i>	
Fuzzing File Systems via Two-Dimensional Input Space Exploration .....	818
<i>Wen Xu (Georgia Institute of Technology), Hyungon Moon (Ulsan National Institute of Science and Technology), Sanidhya Kashyap (Georgia Institute of Technology), Po-Ning Tseng (Georgia Institute of Technology), and Taesoo Kim (Georgia Institute of Technology)</i>	



## Session 10: Side Channels and Data Leakage

F-BLEAU: Fast Black-Box Leakage Estimation .....	835
<i>Giovanni Cherubin (EPFL), Konstantinos Chatzikokolakis (University of Athens), and Catuscia Palamidessi (INRIA, École Polytechnique)</i>	
Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels .....	853
<i>Daniel Genkin (University of Michigan), Mihir Pattani (University of Pennsylvania), Roei Schuster (Tel Aviv University and Cornell Tech), and Eran Tromer (Tel Aviv University and Columbia University)</i>	
Port Contention for Fun and Profit .....	870
<i>Alejandro Cabrera Aldaya (Universidad Tecnológica de la Habana (CUJAE), Habana, Cuba), Billy Bob Brumley (Tampere University, Tampere, Finland), Sohaib ul Hassan (Tampere University, Tampere, Finland), Cesar Pereida García (Tampere University, Tampere, Finland), and Nicola Tuveri (Tampere University, Tampere, Finland)</i>	
Attack Directories, Not Caches: Side Channel Attacks in a Non-Inclusive World .....	888
<i>Mengjia Yan (University of Illinois at Urbana Champaign), Read Sprabery (University of Illinois at Urbana Champaign), Bhargava Gopireddy (University of Illinois at Urbana Champaign), Christopher Fletcher (University of Illinois at Urbana Champaign), Roy Campbell (University of Illinois at Urbana Champaign), and Josep Torrellas (University of Illinois at Urbana Champaign)</i>	
Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone .....	905
<i>Andrew Kwong (University of Michigan), Wenyuan Xu (Zhejiang University), and Kevin Fu (University of Michigan)</i>	

## Session 11: Systems and Applied Security

"Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response .....	920
<i>Elissa M. Redmiles (University of Maryland)</i>	
Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash? .....	935
<i>Yujin Kwon (KAIST), Hyoungshick Kim (Sungkyunkwan University), Jinwoo Shin (KAIST), and Yongdae Kim (KAIST)</i>	
Stealthy Porn: Understanding Real-World Adversarial Images for Illicit Online Promotion .....	952
<i>Kan Yuan (Indiana University Bloomington), Di Tang (Chinese University of Hong Kong), Xiaojing Liao (Indiana University Bloomington), XiaoFeng Wang (Indiana University Bloomington), Xuan Feng (Indiana University Bloomington/Chinese Academy of Sciences), Yi Chen (Indiana University Bloomington/Chinese Academy of Sciences), Menghan Sun (Chinese University of Hong Kong), Haoran Lu (Indiana University Bloomington), and Kehuan Zhang (Chinese University of Hong Kong)</i>	
LBM: A Security Framework for Peripherals within the Linux Kernel .....	967
<i>Dave Jing Tian (University of Florida), Grant Hernandez (University of Florida), Joseph I. Choi (University of Florida), Vanessa Frost (University of Florida), Peter C. Johnson (Middlebury College), and Kevin R. B. Butler (University of Florida)</i>	

SoK: Shining Light on Shadow Stacks .....	985
<i>Nathan Burow (Purdue University), Xinpeng Zhang (Purdue University), and Mathias Payer (EPFL)</i>	
Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers .....	1000
<i>Nolen Scaife (University of Florida), Jasmine Bowers (University of Florida), Christian Peeters (University of Florida), Grant Hernandez (University of Florida), Imani N. Sherman (University of Florida), Patrick Traynor (University of Florida), and Lisa Anthony (University of Florida)</i>	

## Session 12: Cryptography & Encrypted Data

Blind Certificate Authorities .....	1015
<i>Liang Wang (UW Madison), Gilad Asharov (Cornell Tech), Rafael Pass (Cornell Tech), Thomas Ristenpart (Cornell Tech), and Abhi Shelat (Northeastern University)</i>	
Data Recovery on Encrypted Databases with k-Nearest Neighbor Query Leakage .....	1033
<i>Evgenios M. Kornaropoulos (Brown University), Charalampos Papamanthou (University of Maryland), and Roberto Tamassia (Brown University)</i>	
Threshold ECDSA from ECDSA Assumptions: The Multiparty Case .....	1051
<i>Jack Doerner (Northeastern University), Yashvanth Kondi (Northeastern University), Eysa Lee (Northeastern University), and Abhi Shelat (Northeastern University)</i>	
Learning to Reconstruct: Statistical Learning Theory and Encrypted Database Attacks .....	1067
<i>Paul Grubbs (Cornell University), Marie-Sarah Lacharité (Royal Holloway, University of London), Brice Minaud (Ecole Normale Supérieure, CNRS, PSL University and Inria), and Kenneth G. Paterson (Royal Holloway, University of London)</i>	
On the Security of Two-Round Multi-Signatures .....	1084
<i>Manu Drijvers (DFINITY, ETH Zurich), Kasra Edalatnejad (EPFL), Bryan Ford (EPFL), Eike Kiltz (Ruhr-Universität Bochum), Julian Loss (Ruhr-Universität Bochum), Gregory Neven (DFINITY), and Igors Stepanovs (UCSD)</i>	
New Primitives for Actively-Secure MPC over Rings with Applications to Private Machine Learning .....	1102
<i>Ivan Damgård (Aarhus University), Daniel Escudero (Aarhus University), Tore Frederiksen (Alexandra Institute), Marcel Keller (Data61), Peter Scholl (Aarhus University), and Nikolaj Volgushev (Alexandra Institute)</i>	

## Session 13: Network Security

Breaking LTE on Layer Two .....	1121
<i>David Rupperecht (Ruhr-University Bochum), Katharina Kohls (Ruhr-University Bochum), Thorsten Holz (Ruhr-University Bochum), and Christina Pöpper (New York University Abu Dhabi)</i>	

HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows .....	1137
<i>Sadegh Momeni Milajerdi (University of Illinois at Chicago), Rigel Gjomemo (University of Illinois at Chicago), Birhanu Eshete (University of Michigan-Dearborn), R. Sekar (Stony Brook University), and V.N. Venkatakrishnan (University of Illinois at Chicago)</i>	
Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane .....	1153
<i>Hongil Kim (Korea Advanced Institute of Science and Technology (KAIST)), Jiho Lee (Korea Advanced Institute of Science and Technology (KAIST)), Eunkyoo Lee (Korea Advanced Institute of Science and Technology (KAIST)), and Yongdae Kim (Korea Advanced Institute of Science and Technology (KAIST))</i>	
On the Feasibility of Rerouting-Based DDoS Defenses .....	1169
<i>Muoi Tran (National University of Singapore), Min Suk Kang (National University of Singapore), Hsu-Chun Hsiao (National Taiwan University), Wei-Hsuan Chiang (National Taiwan University), Shu-Po Tung (National Taiwan University), and Yu-Su Wang (National Taiwan University)</i>	
Resident Evil: Understanding Residential IP Proxy as a Dark Service .....	1185
<i>Xianghang Mi (Indiana University Bloomington), Xuan Feng (Indiana University Bloomington), Xiaojing Liao (Indiana University Bloomington), Baojun Liu (Tsinghua University), XiaoFeng Wang (Indiana University Bloomington), Feng Qian (Indiana University Bloomington), Zhou Li (IEEE member), Sumayah Alrwais (King Saud University), Limin Sun (Institute of Information Engineering, CAS), and Ying Liu (Tsinghua University)</i>	

## Session 14: Program Languages

Simple High-Level Code for Cryptographic Arithmetic - With Proofs, Without Compromises .....	1202
<i>Andres Erbsen (Massachusetts Institute of Technology), Jade Philipoom (Massachusetts Institute of Technology), Jason Gross (Massachusetts Institute of Technology), Robert Sloan (Massachusetts Institute of Technology), and Adam Chlipala (Massachusetts Institute of Technology)</i>	
SoK: General Purpose Compilers for Secure Multi-Party Computation .....	1220
<i>Marcella Hastings (University of Pennsylvania), Brett Hemenway (University of Pennsylvania), Daniel Noble (University of Pennsylvania), and Steve Zdancewic (University of Pennsylvania)</i>	
The Code That Never Ran: Modeling Attacks on Speculative Evaluation .....	1238
<i>Craig Disselkoen (University of California San Diego, Mozilla Research Internship), Radha Jagadeesan (DePaul University), Alan Jeffrey (Mozilla Research), and James Riely (DePaul University)</i>	
Formally Verified Cryptographic Web Applications in WebAssembly .....	1256
<i>Jonathan Protzenko (Microsoft Research), Benjamin Beurdouche (Inria), Denis Merigoux (Inria), and Karthikeyan Bhargavan (Inria)</i>	

SoK: Sanitizing for Security .....	1275
<i>Dokyung Song (University of California, Irvine), Julian Lettner (University of California, Irvine), Prabhu Rajasekaran (University of California, Irvine), Yeoul Na (University of California, Irvine), Stijn Volckaert (University of California, Irvine), Per Larsen (University of California, Irvine), and Michael Franz (University of California, Irvine)</i>	

## Session 15: Web and Cloud Security

Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps .....	1296
<i>Chaoshun Zuo (The Ohio State University), Zhiqiang Lin (The Ohio State University), and Yinqian Zhang (The Ohio State University)</i>	
Measuring and Analyzing Search Engine Poisoning of Linguistic Collisions .....	1311
<i>Matthew Joslin (University of Texas at Dallas), Neng Li (Shanghai Jiao Tong University), Shuang Hao (University of Texas at Dallas), Minhui Xue (Macquarie University), and Haojin Zhu (Shanghai Jiao Tong University)</i>	
How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples .....	1326
<i>Elissa M. Redmiles (University of Maryland), Sean Kross (University of California San Diego), and Michelle L. Mazurek (University of Maryland)</i>	
PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques against Browser Phishing Blacklists .....	1344
<i>Adam Oest (Arizona State University), Yeganeh Safaei (Arizona State University), Adam Doupé (Arizona State University), Gail-Joon Ahn (Arizona State University, Samsung Research), Brad Wardman (PayPal, Inc.), and Kevin Tyers (PayPal, Inc.)</i>	

## Session 16: IoT Security

SoK: Security Evaluation of Home-Based IoT Deployments .....	1362
<i>Omar Alrawi (Georgia Institute of Technology), Chaz Lever (Georgia Institute of Technology), Manos Antonakakis (Georgia Institute of Technology), and Fabian Monrose (University of North Carolina at Chapel Hill)</i>	
Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems .....	1381
<i>Nan Zhang (Indiana University, Bloomington), Xianghang Mi (Indiana University, Bloomington), Xuan Feng (Indiana University, Bloomington; Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China), XiaoFeng Wang (Indiana University, Bloomington), Yuan Tian (University of Virginia), and Feng Qian (Indiana University, Bloomington)</i>	

Drones' Cryptanalysis - Smashing Cryptography with a Flicker .....	1397
<i>Ben Nassi (Ben-Gurion University of the Negev), Raz Ben-Netanel (Ben-Gurion University of the Negev), Adi Shamir (Weizmann Institute of Science), and Yuval Elovici (Ben-Gurion University of the Negev)</i>	
Dominance as a New Trusted Computing Primitive for the Internet of Things .....	1415
<i>Meng Xu (Georgia Institute of Technology), Manuel Huber (Fraunhofer AISEC), Zhichuang Sun (Northeastern University), Paul England (Microsoft Research), Marcus Peinado (Microsoft Research), Sangho Lee (Microsoft Research), Andrey Marochko (Microsoft Research), Dennis Mattoon (Microsoft Research), Rob Spiger (Microsoft), and Stefan Thom (Microsoft)</i>	

**Author Index**