2021 IEEE Symposium on Security and Privacy (SP 2021)

Virtual Conference
24 – 27 May 2021

Pages 1-658

IEEE Catalog Number: CFP21020-POD
ISBN: 978-1-7281-8935-2

**Copyright © 2021 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:	CFP21020-POD
ISBN (Print-On-Demand):	978-1-7281-8935-2
ISBN (Online):	978-1-7281-8934-5
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
Web:	www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2021 IEEE Symposium on Security and Privacy (SP)

SP 2021

Table of Contents

Message from the General Chair xxi

Message from the Program Chairs xxv

Organizing Committee xxvii

Program Committee xxix

Session 1A: Software Security 1

Using Selective Memoization to Defeat Regular Expression Denial of Service (ReDoS) 1
James C. Davis (Purdue University), Francisco Servant (Virginia Tech), and Dongyoon Lee (Stony Brook University)

Co-Inflow: Coarse-Grained Information Flow Control for Java-like Languages 18
Jian Xiang (Harvard University, USA) and Stephen Chong (Harvard University, USA)

When Function Signature Recovery Meets Compiler Optimization 36
Yan Lin (Singapore Management University) and Debin Gao (Singapore Management University)

Session 1B: Mobile Security 1

How Did That Get In My Phone? Unwanted App Distribution on Android Devices 53
Platon Kotzias (NortonLifeLock Research Group), Juan Caballero (IMDEA Software Institute), and Leyla Bilge (NortonLifeLock Research Group)

Android Custom Permissions Demystified: From Privilege Escalation to Design Shortcomings 70
Rui Li (Shandong University, China), Wenrui Diao (Shandong University, China), Zhou Li (University of California, Irvine, USA), Jianqi Du (Shandong University, China), and Shanqing Guo (Shandong University, China)

Trust, But Verify: A Longitudinal Analysis of Android OEM Compliance and Customization 87
Andrea Possemato (IDEMIA and EURECOM), Simone Aonzo (EURECOM), Davide Balzarotti (EURECOM), and Yanick Fratantonio (EURECOM and Cisco Talos)

Session 1C: Adversarial Machine Learning and Unlearning

Detecting AI Trojans Using Meta Neural Analysis 103
Xiaojun Xu (University of Illinois at Urbana-Champaign, USA), Qi Wang (University of Illinois at Urbana-Champaign, USA), Huichen Li (University of Illinois at Urbana-Champaign, USA), Nikita Borisov (University of Illinois at Urbana-Champaign, USA), Carl A. Gunter (University of Illinois at Urbana-Champaign, USA), and Bo Li (University of Illinois at Urbana-Champaign, USA)

Adversarial Watermarking Transformer: Towards Tracing Text Provenance with Data Hiding 121
Sahar Abdelnabi (CISPA Helmholtz Center for Information Security) and Mario Fritz (CISPA Helmholtz Center for Information Security)

Machine Unlearning 141
Lucas Bourtoule (University of Toronto & Vector Institute, Canada), Varun Chandrasekaran (University of Wisconsin-Madison, USA), Christopher A. Choquette-Choo (University of Toronto & Vector Institute, Canada), Hengrui Jia (University of Toronto & Vector Institute, Canada), Adelin Travers (University of Toronto & Vector Institute, Canada), Baiwu Zhang (University of Toronto & Vector Institute, Canada), David Lie (University of Toronto, Canada), and Nicolas Papernot (University of Toronto & Vector Institute, Canada)

Session 2A: Security of Autonomous Vehicles

Poltergeist: Acoustic Adversarial Machine Learning against Cameras and Computer Vision 160
Xiaoyu Ji (Zhejiang University), Yushi Cheng (Zhejiang University), Yuepeng Zhang (Zhejiang University), Kai Wang (Zhejiang University), Chen Yan (Zhejiang University), Wenyuan Xu (Zhejiang University), and Kevin Fu (University of Michigan)

Invisible for both Camera and LiDAR: Security of Multi-sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks 176
Yulong Cao (University of Michigan), Ningfei Wang (University of California, Irvine), Chaowei Xiao (NVIDIA Research and Arizona State University), Dawei Yang (University of Michigan), Jin Fang (Baidu Research and National Engineering Laboratory of Deep Learning Technology and Application, China), Ruigang Yang (Inceptio), Qi Alfred Chen (University of California, Irvine), Mingyan Liu (University of Michigan), and Bo Li (University of Illinois at Urbana-Champaign)

CANNON: Reliable and Stealthy Remote Shutdown Attacks via Unaltered Automotive Microcontrollers 195
Sekar Kulandaivel (Carnegie Mellon University, USA), Shalabh Jain (Robert Bosch LLC, USA), Jorge Guajardo (Robert Bosch LLC, USA), and Vyas Sekar (Carnegie Mellon University, USA)

Session 2B: Cyber Risk and Abuse

SoK: Quantifying Cyber Risk 211
Daniel W Woods (University of Innsbruck) and Rainer Böhme (University of Innsbruck)

Self-Supervised Euphemism Detection and Identification for Content Moderation 229
Wanzheng Zhu (University of Illinois, at Urbana-Champaign), Hongyu Gong (Facebook), Rohan Bansal (Carnegie Mellon University), Zachary Weinberg (University of Massachusetts, Amherst), Nicolas Christin (Carnegie Mellon University), Giulia Fanti (Carnegie Mellon University), and Suma Bhat (University of Illinois, at Urbana-Champaign)

SoK: Hate, Harassment, and the Changing Landscape of Online Abuse 247
Kurt Thomas (Google), Devdatta Akhawe (Figma, Inc.), Michael Bailey (University of Illinois, Urbana-Champaign), Dan Boneh (Stanford), Elie Bursztein (Google), Sunny Consolvo (Google), Nicola Dell (Cornell Tech), Zakir Durumeric (Stanford), Patrick Gage Kelley (Google), Deepak Kumar (University of Illinois, Urbana-Champaign), Damon McCoy (New York University), Sarah Meiklejohn (University College London), Thomas Ristenpart (Cornell Tech), and Gianluca Stringhini (Boston University)

Session 2C: Crypto Protocols

Keep the Dirt: Tainted TreeKEM, Adaptively and Actively Secure Continuous Group Key Agreement 268
Karen Klein (IST Austria), Guillermo Pascual-Perez (IST Austria), Michael Walter (IST Austria), Chethan Kamath (n/a), Margarita Capretto (Universidad Nacional del Rosario), Miguel Cueto (IST Austria), Ilia Markov (IST Austria), Michelle Yeo (IST Austria), Joël Alwen (Wickr Inc.), and Krzysztof Pietrzak (IST Austria)

Merkle^2: A Low-Latency Transparency Log System 285
Yuncong Hu (UC Berkeley), Kian Hooshmand (UC Berkeley), Harika Kalidhindi (UC Berkeley), Seung Jin Yang (UC Berkeley), and Raluca Ada Popa (UC Berkeley)

Post-Quantum WireGuard 304
Andreas Hülsing (Eindhoven University of Technology), Kai-Chun Ning (KPN B.V.), Peter Schwabe (Max Planck Institute for Security and Privacy & Radboud University), Florian Weber (Eindhoven University of Technology), and Philip R. Zimmermann (Delft University of Technology & KPN B.V.)

Session 3A: Hardware Attacks

Invisible Probe: Timing Attacks with PCIe Congestion Side-channel 322
Mingtian Tan (Fudan University, China), Junpeng Wan (Fudan University, China), Zhe Zhou (Fudan University, China), and Zhou Li (University of California Irvine)

CacheOut: Leaking Data on Intel CPUs via Cache Evictions 339
Stephan van Schaik (University of Michigan), Marina Minkin (University of Michigan), Andrew Kwong (University of Michigan), Daniel Genkin (University of Michigan), and Yuval Yarom (University of Adelaide and Data61)

PLATYPUS: Software-Based Power Side-Channel Attacks on x86 355
Moritz Lipp (Graz University of Technology), Andreas Kogler (Graz University of Technology), David Oswald (University of Birmingham, UK), Michael Schwarz (CISPA Helmholtz Center for Information Security), Catherine Easdon (Graz University of Technology), Claudio Canella (Graz University of Technology), and Daniel Gruss (Graz University of Technology)

Session 3B: Privacy

Defensive Technology Use by Political Activists During the Sudanese Revolution 372
Alaa Daffalla (University of Kansas, USA), Lucy Simko (University of Washington, USA), Tadayoshi Kohno (University of Washington, USA), and Alexandru G. Bardas (University of Kansas, USA)

DP-Sniper: Black-Box Discovery of Differential Privacy Violations using Classifiers 391
Benjamin Bichsel (ETH Zurich, Switzerland), Samuel Steffen (ETH Zurich, Switzerland), Ilija Bogunovic (ETH Zurich, Switzerland), and Martin Vechev (ETH Zurich, Switzerland)

Is Private Learning Possible with Instance Encoding? 410
Nicholas Carlini (Google), Samuel Deng (Columbia University), Sanjam Garg (UC Berkeley), Somesh Jha (University of Wisconsin), Saeed Mahloujifar (Princeton University), Mohammad Mahmoody (University of Virginia), Abhradeep Thakurta (Google), and Florian Tramer (Stanford University)

Session 3C: Crypto Currencies 1

High-Frequency Trading on Decentralized On-chain Exchanges 428
Liyi Zhou (Imperial College London, United Kingdom), Kaihua Qin (Imperial College London, United Kingdom), Christof Ferreira Torres (University of Luxembourg, Luxembourg), Duc V Le (Purdue University, United States), and Arthur Gervais (Imperial College London, United Kingdom)

Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma 446
Joachim Neu (Stanford University, USA), Ertem Nusret Tas (Stanford University, USA), and David Tse (Stanford University, USA)

Red Belly: A Secure, Fair and Scalable Open Blockchain 466
Tyler Crain (University of Sydney), Christopher Natoli (University of Sydney), and Vincent Gramoli (University of Sydney and CSIRO)

Session 4A: IoT Security and Privacy

DIANE: Identifying Fuzzing Triggers in Apps to Generate Under-constrained Inputs for IoT Devices 484
Nilo Redini (UC Santa Barbara), Andrea Continella (University of Twente), Dipanjan Das (UC Santa Barbara), Giulio De Pasquale (UC Santa Barbara), Noah Spahn (UC Santa Barbara), Aravind Machiry (Purdue University), Antonio Bianchi (Purdue University), Christopher Kruegel (UC Santa Barbara), and Giovanni Vigna (UC Santa Barbara)

Data Privacy in Trigger-Action Systems 501
Yunang Chen (University of Wisconsin-Madison), Amrita Roy Chowdhury (University of Wisconsin-Madison), Ruizhe Wang (University of Wisconsin-Madison), Andrei Sabelfeld (Chalmers University of Technology), Rahul Chatterjee (University of Wisconsin-Madison), and Earlence Fernandes (University of Wisconsin-Madison)

Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices? 519
Pardis Emami-Naeini (University of Washington), Janarth Dheenadhayalan (Carnegie Mellon University), Yuvraj Agarwal (Carnegie Mellon University), and Lorrie Faith Cranor (Carnegie Mellon University)

Session 4B: Formal Verification of Protocols

An Interactive Prover for Protocol Verification in the Computational Model 537
David Baelde (LMF, ENS Paris-Saclay & CNRS, Université Paris-Saclay, France), Stéphanie Delaune (Univ Rennes, CNRS, IRISA, France), Charlie Jacomme (CISPA Helmholtz Center for Information Security, Germany), Adrien Koutsos (Inria Paris, France), and Solène Moreau (Univ Rennes, CNRS, IRISA, France)

SmartPulse: Automated Checking of Temporal Properties in Smart Contracts 555
Jon Stephens (The University of Texas at Austin), Kostas Ferles (The University of Texas at Austin), Benjamin Mariano (The University of Texas at Austin), Shuvendu Lahiri (Microsoft Research), and Isil Dillig (The University of Texas at Austin)

An I/O Separation Model for Formal Verification of Kernel Implementations 572
Miao Yu (Carnegie Mellon University), Virgil Gligor (Carnegie Mellon University), and Limin Jia (Carnegie Mellon University)

Session 4C: Distributed Cryptography

Diogenes: Lightweight Scalable RSA Modulus Generation with a Dishonest Majority 590
Megan Chen (Northeastern University & Ligero Inc.), Carmit Hazay (Bar-Ilan University & Ligero Inc.), Yuval Ishai (Technion University), Yuriy Kashnikov (Ligero Inc.), Daniele Micciancio (UC San Diego), Tarik Riviere (Ligero Inc.), Abhi Shelat (Northeastern University & Ligero Inc.), Muthuramakrishnan Venkitasubramaniam (University of Rochester & Ligero Inc.), and Ruihan Wang (Ligero Inc.)

Refresh When You Wake Up: Proactive Threshold Wallets with Offline Devices 608
Yashvanth Kondi (Northeastern University), Bernardo Magri (Concordium Blockchain Research Center, Aarhus University), Claudio Orlandi (Aarhus University), and Omer Shlomovits (KZen Research)

Compact Certificates of Collective Knowledge 626
Silvio Micali (Algorand and MIT, USA), Leonid Reyzin (Algorand and Boston University, USA), Georgios Vlachos (Axelar and University of Waterloo, Canada), Rias S. Wahby (Algorand and Stanford University, USA), and Nickolai Zeldovich (Algorand and MIT, USA)

Session 5A: Fuzzing

One Engine to Fuzz 'em All: Generic Language Processor Testing with Semantic Validation 642
Yongheng Chen (Georgia Institute of Technology, USA), Rui Zhong (Pennsylvania State University, USA), Hong Hu (Pennsylvania State University, USA), Hangfan Zhang (Pennsylvania State University), Yupeng Yang (University of Electronic Science and Technology of China, China), Dinghao Wu (Pennsylvania State University, USA), and Wenke Lee (Georgia Institute of Technology, USA)

STOCHFUZZ: Sound and Cost-effective Fuzzing of Stripped Binaries by Incremental and Stochastic Rewriting 659
Zhuo Zhang (Purdue University, USA), Wei You (Renmin University of China, China), Guanhong Tao (Purdue University, USA), Yousra Aafer (University of Waterloo, Canada), Xuwei Liu (Purdue University, USA), and Xiangyu Zhang (Purdue University, USA)

NTFUZZ: Enabling Type-Aware Kernel Fuzzing on Windows with Static Binary Analysis 677
Jaeseung Choi (KAIST, Korea), Kangsu Kim (KAIST, Korea), Daejin Lee (KAIST, Korea), and Sang Kil Cha (KAIST, Korea)

Session 5B: Attacks on Speech Systems

Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems 694
Guangke Chen (ShanghaiTech University; Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Sen Chen (Tianjin University; Nanyang Technological University), Lingling Fan (Nanyang Technological University), Xiaoning Du (Nanyang Technological University), Zhe Zhao (ShanghaiTech University), Fu Song (ShanghaiTech University; Shanghai Engineering Research Center of Intelligent Vision and Imaging), and Yang Liu (Nanyang Technological University)

Hear "No Evil", See "Kenansville": Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems 712
Hadi Abdullah (University of Florida), Muhammad Sajidur Rahman (University of Florida), Washington Garcia (University of Florida), Kevin Warren (University of Florida), Anurag Swarnim Yadav (University of Florida), Tom Shrimpton (University of Florida), and Patrick Traynor (University of Florida)

SoK: The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems 730
Hadi Abdullah (University of Florida), Kevin Warren (University of Florida), Vincent Bindschaedler (University of Florida), Nicolas Papernot (University of Toronto), and Patrick Traynor (University of Florida)

Session 5C: Cryptography 1

Cross-Domain Access Control Encryption: Arbitrary-Policy, Constant-Size, Efficient 748
Xiuhua Wang (The Chinese University of Hong Kong) and Sherman S. M. Chow (The Chinese University of Hong Kong)

Lightweight Techniques for Private Heavy Hitters 762
Dan Boneh (Stanford), Elette Boyle (IDC Herzliya), Henry Corrigan-Gibbs (MIT CSAIL), Niv Gilboa (Ben-Gurion University), and Yuval Ishai (Technion)

SoK: Computer-Aided Cryptography 777
Manuel Barbosa (University of Porto and INESC TEC, Portugal), Gilles Barthe (Max Planck Institute for Security and Privacy, Germany and IMDEA Software Institute, Spain), Karthik Bhargavan (INRIA Paris, France), Bruno Blanchet (INRIA Paris, France), Cas Cremers (CISPA Helmholtz Center for Information Security, Germany), Kevin Liao (Max Planck Institute for Security and Privacy, Germany and Massachusetts Institute of Technology, USA), and Bryan Parno (Carnegie Mellon University, USA)

Session 6A: Software Security 2

ConDySTA: Context-Aware Dynamic Supplement to Static Taint Analysis 796
Xueling Zhang (University of Texas at San Antonio, USA), Xiaoyin Wang (University of Texas at San Antonio, USA), Rocky Slavin (University of Texas at San Antonio, USA), and Jianwei Niu (University of Texas at San Antonio, USA)

OSPREY: Recovery of Variable and Data Structure via Probabilistic Analysis for Stripped Binary 813
Zhuo Zhang (Purdue University, USA), Yapeng Ye (Purdue University, USA), Wei You (Renmin University of China, China), Guanhong Tao (Purdue University, USA), Wen-chuan Lee (Purdue University, USA), Yonghwi Kwon (University of Virginia, USA), Yousra Aafer (University of Waterloo, Canada), and Xiangyu Zhang (Purdue University, USA)

SoK: All You Ever Wanted to Know About x86/x64 Binary Disassembly but Were Afraid to Ask 833
Chengbin Pang (Stevens Institute of Technology, USA; Nanjing University, China), Ruotong Yu (Stevens Institute of Technology, USA), Yaohui Chen (Facebook Inc., USA), Eric Koskinen (Stevens Institute of Technology, USA), Georgios Portokalidis (Stevens Institute of Technology, USA), Bing Mao (Nanjing University, China), and Jun Xu (Stevens Institute of Technology, USA)

Session 6B: Differential Privacy

Learning Differentially Private Mechanisms 852
Subhajit Roy (Indian Institute of Technology Kanpur, India), Justin Hsu (University of Wisconsin–Madison, USA), and Aws Albarghouthi (University of Wisconsin–Madison, USA)

Adversary Instantiation: Lower Bounds for Differentially Private Machine Learning 866
Milad Nasr (University of Massachusetts Amherst), Shuang Song (Google Brain), Abhradeep Thakurta (Google Brain), Nicolas Papernot (Google Brain), and Nicholas Carlini (Google Brain)

Manipulation Attacks in Local Differential Privacy 883
Albert Cheu (Northeastern University), Adam Smith (Boston University), and Jonathan Ullman (Northeastern University)

Session 6C: Crypto Currencies 2

Bitcoin-Compatible Virtual Channels 901
Lukas Aumayr (TU Wien, Austria), Oğuzhan Ersoy (TU Delft, Netherlands), Andreas Erwig (TU Darmstadt, Germany), Sebastian Faust (TU Darmstadt, Germany), Kristina Hostáková (ETH Zürich, Switzerland), Matteo Maffei (TU Wien, Austria), Pedro Moreno-Sanchez (IMDEA Software Institute, Spain), and Siavash Riahi (TU Darmstadt, Germany)

On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols 919
Liyi Zhou (Imperial College London), Kaihua Qin (Imperial College London), Antoine Cully (Imperial College London), Benjamin Livshits (Imperial College London), and Arthur Gervais (Imperial College London)

Lockable Signatures for Blockchains: Scriptless Scripts for All Signatures 937
Sri Aravinda Krishnan Thyagarajan (Friedrich Alexander Universität Erlangen-Nürnberg, Germany) and Giulio Malavolta (Max Planck Institute for Security and Privacy, Germany)

Session 7A: HW Security

Randomized Last-Level Caches are Still Vulnerable to Cache Side-Channel Attacks! But We Can Fix It 955
Wei Song (State Key Laboratory of Information Security, Institute of Information Engineering, CAS), Boya Li (State Key Laboratory of Information Security, Institute of Information Engineering, CAS), Zihan Xue (State Key Laboratory of Information Security, Institute of Information Engineering, CAS), Zhenzhen Li (State Key Laboratory of Information Security, Institute of Information Engineering, CAS), Wenhao Wang (State Key Laboratory of Information Security, Institute of Information Engineering, CAS), and Peng Liu (Pennsylvania State University)

Bomberman: Defining and Defeating Hardware Ticking Timebombs at Design-Time 970
Timothy Trippel (University of Michigan), Kang G. Shin (University of Michigan), Kevin B. Bush (MIT Lincoln Laboratory), and Matthew Hicks (Virginia Tech)

Systematic Analysis of Randomization-Based Protected Cache Architectures 987
Antoon Purnal (imec-COSIC, KU Leuven), Lukas Giner (Graz University of Technology), Daniel Gruss (Graz University of Technology), and Ingrid Verbauwhede (imec-COSIC, KU Leuven)

Session 7B: ML Security and Privacy

SIRNN: A Math Library for Secure RNN Inference .1003
Deevashwer Rathee (Microsoft Research, India), Mayank Rathee (Microsoft Research, India), Rahul Kranti Kiran Goli (Microsoft Research, India), Divya Gupta (Microsoft Research, India), Rahul Sharma (Microsoft Research, India), Nishanth Chandran (Microsoft Research, India), and Aseem Rastogi (Microsoft Research, India)

CryptGPU: Fast Privacy-Preserving Machine Learning on the GPU .1021
Sijun Tan (University of Virginia), Brian Knott (Facebook AI Research), Yuan Tian (University of Virginia), and David J. Wu (University of Virginia)

Proof-of-Learning: Definitions and Practice .1039
Hengrui Jia (University of Toronto and Vector Institute), Mohammad Yaghini (University of Toronto and Vector Institute), Christopher A. Choquette-Choo (University of Toronto and Vector Institute), Natalie Dullerud (University of Toronto and Vector Institute), Anvith Thudi (University of Toronto and Vector Institute), Varun Chandrasekaran (University of Wisconsin-Madison), and Nicolas Papernot (University of Toronto and Vector Institute)

Session 7C: Secure Multiparty Computation and Homomorphic Encryption

PEGASUS: Bridging Polynomial and Non-polynomial Evaluations in Homomorphic Encryption .1057
Wen-jie Lu (Alibaba Group, China), Zhicong Huang (Alibaba Group, China), Cheng Hong (Alibaba Group, China), Yiping Ma (University of Pennsylvania, USA), and Hunter Qu (Alibaba Group)

Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits .1074
Chenkai Weng (Northwestern University), Kang Yang (State Key Laboratory of Cryptology), Jonathan Katz (University of Maryland), and Xiao Wang (Northwestern University)

SoK: Fully Homomorphic Encryption Compilers .1092
Alexander Viand (ETH Zurich, Switzerland), Patrick Jattke (ETH Zurich, Switzerland), and Anwar Hithnawi (ETH Zurich, Switzerland)

Session 8A: Web Security 1

CrawlPhish: Large-Scale Analysis of Client-Side Cloaking Techniques in Phishing .1109
Penghui Zhang (Arizona State University), Adam Oest (Arizona State University and PayPal, Inc.), Haehyun Cho (Arizona State University), Zhibo Sun (Arizona State University), RC Johnson (PayPal, Inc.), Brad Wardman (PayPal, Inc.), Shaown Sarker (North Carolina State University), Alexandros Kapravelos (North Carolina State University), Tiffany Bao (Arizona State University), Ruoyu Wang (Arizona State University), Yan Shoshitaishvili (Arizona State University), Adam Doupé (Arizona State University), and Gail-Joon Ahn (Arizona State University and Samsung Research)

Black Widow: Blackbox Data-driven Web Scanning .1125..

Benjamin Eriksson (Chalmers University of Technology, Sweden), Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany), and Andrei Sabelfeld (Chalmers University of Technology, Sweden)

Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors .1143......

Umar Iqbal (The University of Iowa), Steven Englehardt (Mozilla Corporation), and Zubair Shafiq (University of California, Davis)

Session 8B: Network Security

A Security Model and Fully Verified Implementation for the IETF QUIC Record Layer .1162........

Antoine Delignat-Lavaud (Microsoft Research), Cédric Fournet (Microsoft Research), Bryan Parno (Carnegie Mellon University), Jonathan Protzenko (Microsoft Research), Tahina Ramananandro (Microsoft Research), Jay Bosamiya (Carnegie Mellon University), Joseph Lallemand (INRIA Nancy Grand-Est), Itsaka Rakotonirina (Loria, INRIA Nancy Grand-Est), and Yi Zhou (Carnegie Mellon University)

Cross Layer Attacks and How to Use Them (for DNS Cache Poisoning, Device Tracking and More) .1179...

Amit Klein (Bar-Ilan University, Israel)

Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis ......
1197

Yi Chen (Indiana University Bloomington), Yepeng Yao (Institute of Information Engineering, CAS), XiaoFeng Wang (Indiana University Bloomington), Dandan Xu (Institute of Information Engineering, CAS), Chang Yue (Institute of Information Engineering, CAS), Xiaozhong Liu (Indiana University Bloomington), Kai Chen (Institute of Information Engineering, CAS), Haixu Tang (Indiana University Bloomington), and Baoxu Liu (Institute of Information Engineering, CAS)

Session 8C: Smart Contracts

sGUARD: Towards Fixing Vulnerable Smart Contracts Automatically .1215................................

Tai Duy Nguyen (Singapore Management University, Singapore), Long Hong Pham (Singapore Management University, Singapore), and Jun Sun (Singapore Management University, Singapore)

MAD-HTLC: Because HTLC is Crazy-Cheap to Attack .1230...

Itay Tsabary (Technion, Israel), Matan Yechieli (Technion, Israel), Alex Manuskin (ZenGo-X, Israel), and Ittay Eyal (Technion, Israel)

Compositional Security for Reentrant Applications .1249...

Ethan Cecchetti (Cornell University), Siqiu Yao (Cornell University), Haobin Ni (Cornell University), and Andrew Myers (Cornell University)

Session 9A: Vulnerabilities

HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises .1268
Daniel Votipka (Tufts University), Eric Zhang (University of Maryland), and Michelle Mazurek (University of Maryland)

DiFuzzRTL: Differential Fuzz Testing to Find CPU Bugs .1286
Jaewon Hur (Seoul National University), Suhwan Song (Seoul National University), Dongup Kwon (Seoul National University), Eunjin Baek (Seoul National University), Jangwoo Kim (Seoul National University), and Byoungyoung Lee (Seoul National University)

Session 9B: Wireless and Electromagnetic Channels

When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient .1304
Cheng Shen (Peking University), Tian Liu (Peking University), Jun Huang (Massachusetts Institute of Technology), and Rui Tan (Nanyang Technological University)

Linking Bluetooth LE & Classic and Implications for Privacy-Preserving Bluetooth-Based Protocols .1318
Norbert Ludant (Northeastern University, USA), Tien D. Vo-Huu (Northeastern University, USA), Sashank Narain (University of Massachusetts Lowell, USA), and Guevara Noubir (Northeastern University, USA)

Method Confusion Attack on Bluetooth Pairing .1332
Maximilian von Tschirschnitz (Technical University Munich), Ludwig Peuckert (Technical University Munich), Fabian Franzen (Technical University Munich), and Jens Grossklags (Technical University Munich)

Session 9C: Authentication, Identity and Access Control

CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability .1348
Deepak Maram (Cornell Tech, USA), Harjasleen Malvai (Cornell University, USA), Fan Zhang (Cornell Tech, USA), Nerla Jean-Louis (University of Illinois at Urbana-Champaign, USA), Alexander Frolov (Cornell University, USA), Tyler Kell (Cornell Tech, USA), Tyrone Lobban (J.P. Morgan, USA), Christine Moy (J.P. Morgan, USA), Ari Juels (Cornell Tech, USA), and Andrew Miller (University of Illinois at Urbana-Champaign, USA)

They Would do Better if They Worked Together: The Case of Interaction Problems Between Password Managers and Websites .1367
Nicolas Huaman (CISPA Helmholtz Center for Information Security), Sabrina Amft (Leibniz Universität Hannover), Marten Oltrogge (CISPA Helmholtz Center for Information Security), Yasemin Acar (Max Planck Institute for Security and Privacy), and Sascha Fahl (CISPA Helmholtz Center for Information Security)

Improving Password Guessing via Representation Learning 1382
Dario Pasquini (Sapienza University of Rome, Italy / Stevens Institute of Technology, USA / Institute of Applied Computing, CNR, Italy), Ankit Gangwal (University of Padua, Italy / Stevens Institute of Technology, USA), Giuseppe Ateniese (Stevens Institute of Technology, USA), Massimo Bernaschi (Institute of Applied Computing CNR, Italy), and Mauro Conti (University of Padua, Italy)

Session 10A: Program Security and Cyber-Physical Systems

ARBITRAR: User-Guided API Misuse Detection 1400
Ziyang Li (University of Pennsylvania), Aravind Machiry (Purdue University), Binghong Chen (Georgia Institute of Technology), Mayur Naik (University of Pennsylvania), Ke Wang (Visa Research), and Le Song (Georgia Institute of Technology)

Compositional Non-Interference for Fine-Grained Concurrent Programs 1416
Dan Frumin (Radboud University, Netherlands), Robbert Krebbers (TU Delft, Netherlands), and Lars Birkedal (Aarhus University, Denmark)

SoK: Security and Privacy in the Age of Commercial Drones 1434
Ben Nassi (Ben-Gurion University of the Negev), Ron Bitton (Ben-Gurion University of the Negev), Ryusuke Masuoka (Fujitsu System Integration Laboratories), Asaf Shabtai (Ben-Gurion University of the Negev), and Yuval Elovici (Ben-Gurion University of the Negev)

Session 10B: Web Attacks

A First Look at Zoombombing 1452
Chen Ling (Boston University), Utcukan Balcı (Binghamton University), Jeremy Blackburn (Binghamton University), and Gianluca Stringhini (Boston University)

Revealer: Detecting and Exploiting Regular Expression Denial-of-Service Vulnerabilities 1468
Yinxi Liu (Chinese University of Hong Kong), Mingxue Zhang (Chinese University of Hong Kong), and Wei Meng (Chinese University of Hong Kong)

Breaking the Specification: PDF Certification 1485
Simon Rohlmann (Ruhr University Bochum, Germany), Vladislav Mladenov (Ruhr University Bochum, Germany), Christian Mainka (Ruhr University Bochum, Germany), and Jörg Schwenk (Ruhr University Bochum, Germany)

Session 10C: Crypto Applications and Attacks

Response-Hiding Encrypted Ranges: Revisiting Security via Parametrized Leakage-Abuse Attacks 1502
Evgenios M. Kornaropoulos (UC Berkeley, USA), Charalampos Papamanthou (University of Maryland, USA), and Roberto Tamassia (Brown University, USA)

A Decentralized and Encrypted National Gun Registry 1520
Seny Kamara (Brown University), Tarik Moataz (Aroki Systems), Andrew Park (Brown University), and Lucy Qin (Brown University)

Zero Knowledge for Everything and Everyone: Fast ZK Processor with Cached ORAM for ANSI C Programs 1538
David Heath (Georgia Institute of Technology), Yibin Yang (Georgia Institute of Technology), David Devecsery (Georgia Institute of Technology), and Vladimir Kolesnikov (Georgia Institute of Technology)

Session 11A: Malware and Attacks

Survivalism: Systematic Analysis of Windows Malware Living-Off-the-Land 1557
Frederick Barr-Smith (Oxford University), Xabier Ugarte-Pedrero (Cisco Systems), Mariano Graziano (Cisco Systems), Riccardo Spolaor (Oxford University), and Ivan Martinovic (Oxford University)

Runtime Recovery of Web Applications under Zero-Day ReDoS Attacks 1575
Zhihao Bai (Johns Hopkins University, USA), Ke Wang (Peking University, China), Hang Zhu (Johns Hopkins University, USA), Yinzhi Cao (Johns Hopkins University, USA), and Xin Jin (Peking University, China)

Good Bot, Bad Bot: Characterizing Automated Browsing Activity 1589
Xigao Li (Stony Brook University, USA), Babak Amin Azad (Stony Brook University, USA), Amir Rahmati (Stony Brook University, USA), and Nick Nikiforakis (Stony Brook University, USA)

Session 11B: Mobile Security 2

Trouble Over-the-Air: An Analysis of FOTA Apps in the Android Ecosystem 1606
Eduardo Blázquez (Universidad Carlos III de Madrid, Spain), Sergio Pastrana (Universidad Carlos III de Madrid, Spain), Álvaro Feal (IMDEA Networks Institute, Spain / Universidad Carlos III de Madrid, Spain), Julien Gamba (IMDEA Networks Institute, Spain / Universidad Carlos III de Madrid, Spain), Platon Kotzias (NortonLifelock Research Group, France), Narseo Vallina-Rodriguez (IMDEA Networks Institute, Spain / ICSI, USA / AppCensus Inc., USA), and Juan Tapiador (Universidad Carlos III de Madrid, Spain)

Doing Good by Fighting Fraud: Ethical Anti-fraud Systems for Mobile Payments 1623
Zainul Abi Din (University of California, Davis), Hari Venugopalan (University of California, Davis), Henry Lin (Bouncer Technologies), Adam Wushensky (Bouncer Technologies), Steven Liu (Bouncer Technologies), and Samuel T. King (University of California, Davis and Bouncer Technologies)

Happer: Unpacking Android Apps via a Hardware-Assisted Approach 1641
Lei Xue (The Hong Kong Polytechnic University), Hao Zhou (The Hong Kong Polytechnic University), Xiapu Luo (The Hong Kong Polytechnic University), Yajin Zhou (Zhejiang University), Yang Shi (Tongji University), Guofei Gu (Texas A&M University), Fengwei Zhang (Southern University of Science and Technology), and Man Ho Au (The University of Hong Kong)

Session 11C: Signature Schemes

The Provable Security of Ed25519: Theory and Practice .1659..
Jacqueline Brendel (CISPA Helmholtz Center for Information Security, Germany), Cas Cremers (CISPA Helmholtz Center for Information Security, Germany), Dennis Jackson (ETH Zurich, Switzerland), and Mang Zhao (CISPA Helmholtz Center for Information Security, Germany)

Epochal Signatures for Deniable Group Chats .1677...
Andreas Hülsing (TU Eindhoven, The Netherlands) and Florian Weber (TU Eindhoven, The Netherlands)

BUFFing Signature Schemes beyond Unforgeability and the Case of Post-Quantum Signatures .1696
Cas Cremers (CISPA Helmholtz Center for Information Security, Germany), Samed Düzlü (Technische Universität Darmstadt, Germany), Rune Fiedler (Technische Universität Darmstadt, Germany), Christian Janson (Technische Universität Darmstadt, Germany), and Marc Fischlin (Technische Universität Darmstadt, Germany)

Session 12A: Web Security 2

Detecting Filter List Evasion with Event-Loop-Turn Granularity JavaScript Signatures .1715.........
Quan Chen (North Carolina State University, USA), Peter Snyder (Brave Software, USA), Ben Livshits (Brave Software, USA), and Alexandros Kapravelos (North Carolina State University, USA)

Reading between the Lines: An Extensive Evaluation of the Security and Privacy Implications of EPUB Reading Systems .1730...
Gertjan Franken (imec-DistriNet, KU Leuven), Tom Van Goethem (imec-DistriNet, KU Leuven), and Wouter Joosen (imec-DistriNet, KU Leuven)

Session 12B: Formal Methods in the Real World

Did You Mix Me? Formally Verifying Verifiable Mix Nets in Electronic Voting .1748....................
Thomas Haines (Norwegian University of Science and Technology, Norway), Rajeev Goré (The Australian National University, Australia), and Bhavesh Sharma (The Australian National University, Australia)

The EMV Standard: Break, Fix, Verify .1766...
David Basin (ETH Zurich, Switzerland), Ralf Sasse (ETH Zurich, Switzerland), and Jorge Toro-Pozo (ETH Zurich, Switzerland)

A Secure and Formally Verified Linux KVM Hypervisor .1782..
Shih-Wei Li (Columbia University), Xupeng Li (Columbia University), Ronghui Gu (Columbia University), Jason Nieh (Columbia University), and John Zhuang Hui (Columbia University)

Session 12C: Anonymity in Crypto Currencies

Many-out-of-Many Proofs and Applications to Anonymous Zether 1800
Benjamin E. Diamond (J.P. Morgan AI Research)

On the Anonymity Guarantees of Anonymous Proof-of-Stake Protocols 1818
Markulf Kohlweiss (University of Edinburgh), Varun Madathil (North Carolina State University), Kartik Nayak (Duke University), and Alessandra Scafuro (North Carolina State University)

A2L: Anonymous Atomic Locks for Scalability in Payment Channel Hubs 1834
Erkan Tairi (TU Wien), Pedro Moreno-Sanchez (IMDEA Software Institute), and Matteo Maffei (TU Wien)

Session 13A: HW Side Channels and Defenses

CrossTalk: Speculative Data Leaks across Cores are Real 1852
Hany Ragab (Vrije Universiteit Amsterdam, The Netherlands), Alyssa Milburn (Vrije Universiteit Amsterdam, The Netherlands), Kaveh Razavi (ETH Zurich, Switzerland), Herbert Bos (Vrije Universiteit Amsterdam, The Netherlands), and Cristiano Giuffrida (Vrije Universiteit Amsterdam, The Netherlands)

Hardware-Software Contracts for Secure Speculation 1868
Marco Guarnieri (IMDEA Software Institute), Boris Köpf (Microsoft Research), Jan Reineke (Saarland University), and Pepe Vila (IMDEA Software Institute)

High-Assurance Cryptography in the Spectre Era 1884
Gilles Barthe (Max Planck Institute for Security and Privacy, Germany and IMDEA Software Institute, Spain), Sunjay Cauligi (University of California, San Diego, USA), Benjamin Gregoire (INRIA Sophia Antipolis, Paris), Adrien Koutsos (INRIA Paris, France), Kevin Liao (Max Planck Institute for Security and Privacy, Germany and Massachusetts Institute of Technology, USA), Tiago Oliveira (University of Porto, Portugal and INESC TEC, Portugal), Swarn Priya (Purdue University, USA), Tamara Rezk (INRIA Sophia Antipolis, France), and Peter Schwabe (Max Planck Institute for Security and Privacy, Germany)

Session 13B: Dynamic Analysis

A Novel Dynamic Analysis Infrastructure to Instrument Untrusted Execution Flow Across User-Kernel Spaces 1902
Jiaqi Hong (Singapore Management University) and Xuhua Ding (Singapore Management University)

DynPTA: Combining Static and Dynamic Analysis for Practical Selective Data Protection 1919
Tapti Palit (Stony Brook University, USA), Jarin Firose Moon (Stony Brook University, USA), Fabian Monrose (UNC Chapel Hill, USA), and Michalis Polychronakis (Stony Brook University, USA)

DICE: Automatic Emulation of DMA Input Channels for Dynamic Firmware Analysis 1938
Alejandro Mera (Northeastern University, USA), Bo Feng (Northeastern University, USA), Long Lu (Northeastern University, USA), Engin Kirda (Northeastern University, USA), and William Robertson (Northeastern University, USA)

Session 13C: Cryptography 2

Real-World Snapshots vs. Theory: Questioning the t-Probing Security Model 1955
Thilo Krachenfels (Technische Universität Berlin), Fatemeh Ganji (Worcester Polytechnic Institute), Amir Moradi (Ruhr-Universität Bochum), Shahin Tajik (Worcester Polytechnic Institute), and Jean-Pierre Seifert (Technische Universität Berlin)

CRYLOGGER: Detecting Crypto Misuses Dynamically 1972
Luca Piccolboni (Columbia University, USA), Giuseppe Di Guglielmo (Columbia University, USA), Luca P. Carloni (Columbia University, USA), and Simha Sethumadhavan (Columbia University, USA)

Author Index