2020 IEEE Symposium on Security and Privacy (SP 2020)

San Francisco, California, USA
18-21 May 2020

Pages 1-876

IEEE Catalog Number: CFP20020-POD
ISBN: 978-1-7281-3498-7

Copyright © 2020 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:	CFP20020-POD
ISBN (Print-On-Demand):	978-1-7281-3498-7
ISBN (Online):	978-1-7281-3497-0
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

2020 IEEE Symposium on Security and Privacy SP 2020

Table of Contents

Message from the General Chair xx
Message from the Program Chairs xxiii
Organizing Committee xxiv

Session #1: Microarchitectural Security

SPECTECTOR: Principled Detection of Speculative Information Flows 1
Marco Guarnieri (IMDEA Software Institute), Boris Köpf (Microsoft Research), José F. Morales (IMDEA Software Institute), Jan Reineke (Saarland University), and Andrés Sánchez (IMDEA Software Institute)

NetCAT: Practical Cache Attacks from the Network 20
Michael Kurth (Vrije Universiteit Amsterdam, The Netherlands ; ETH Zurich, Switzerland), Ben Gras (Vrije Universiteit Amsterdam, The Netherlands), Dennis Andriesse (Vrije Universiteit Amsterdam, The Netherlands), Cristiano Giuffrida (Vrije Universiteit Amsterdam, The Netherlands), Herbert Bos (Vrije Universiteit Amsterdam, The Netherlands), and Kaveh Razavi (Vrije Universiteit Amsterdam, The Netherlands)

SPECCFI: Mitigating Spectre Attacks Using CFI Informed Speculation 39
Esmaeil Mohammadian Koruyeh (University of California Riverside), Shirin Haji Amin Shirazi (University of California Riverside), Khaled N. Khasawneh (George Mason University), Chengyu Song (University of California Riverside), and Nael Abu-Ghazaleh (University of California Riverside)

LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection 54
Jo Van Bulck (imec-DistriNet, KU Leuven), Daniel Moghimi (Worcester Polytechnic Institute), Michael Schwarz (Graz University of Technology), Moritz Lipp (Graz University of Technology), Marina Minkin (University of Michigan), Daniel Genkin (University of Michigan), Yuval Yarom (University of Adelaide and Data61), Berk Sunar (Worcester Polytechnic Institute), Daniel Gruss (Graz University of Technology), and Frank Piessens (imec-DistriNet, KU Leuven)

Session #1: Blockchain I

HydRand: Efficient Continuous Distributed Randomness 73
Philipp Schindler (SBA Research), Aljosha Judmayer (SBA Research), Nicholas Stifter (SBA Research / TU Wien), and Edgar Weippl (SBA Research / TU Wien)

OHIE: Blockchain Scaling Made Simple 90
Haifeng Yu (National University of Singapore), Ivica Nikolic (National University of Singapore), Ruomu Hou (National University of Singapore), and Prateek Saxena (National University of Singapore)

Sync HotStuff: Simple and Practical Synchronous State Machine Replication 106
Ittai Abraham (VMware Research), Dahlia Malkhi (Calibra), Kartik Nayak (Duke University), Ling Ren (University of Illinois at Urbana-Champaign), and Maofan Yin (Cornell University)

Replicated State Machines without Replicated Execution 119
Jonathan Lee (Microsoft Research), Kirill Nikitin (EPFL), and Srinath Setty (Microsoft Research)

Session #1: Anonymity and Censorship

ICLab: A Global, Longitudinal Internet Censorship Measurement Platform 135
Arian Akhavan Niaki (University of Massachusetts, Amherst), Shinyoung Cho (University of Massachusetts, Amherst / Stony Brook University), Zachary Weinberg (Carnegie Mellon University), Nguyen Phong Hoang (Stony Brook University), Abbas Razaghpanah (Stony Brook University), Nicolas Christin (Carnegie Mellon University), and Phillipa Gill (Stony Brook University)

High Precision Open-World Website Fingerprinting 152
Tao Wang (Hong Kong University of Science and Technology)

Breaking and (Partially) Fixing Provably Secure Onion Routing 168
Christiane Kuhn (KIT Karlsruhe), Martin Beck (TU Dresden), and Thorsten Strufe (KIT Karlsruhe and TU Dresden)

Are Anonymity-Seekers Just like Everybody Else? An Analysis of Contributions to Wikipedia from Tor 186
Chau Tran (New York University), Kaylea Champion (University of Washington), Andrea Forte (Drexel University), Benjamin Mako Hill (University of Washington), and Rachel Greenstadt (New York University)

Session #2: Sensors and Emanations

Detection of Electromagnetic Interference Attacks on Sensor Systems 203
Youqian ZHANG (University of Oxford) and Kasper Rasmussen (University of Oxford)

WaveSpy: Remote and Through-wall Screen Attack via mmWave Sensing .217

Zhengxiong Li (University at Buffalo, SUNY), Fenglong Ma (University at Buffalo, SUNY), Aditya Singh Rathore (University at Buffalo, SUNY), Zhuolin Yang (University at Buffalo, SUNY), Baicheng Chen (University at Buffalo, SUNY), Lu Su (University at Buffalo, SUNY), and Wenyao Xu (University at Buffalo, SUNY)

SoK: A Minimalist Approach to Formalizing Analog Sensor Security .233

Chen Yan (Zhejiang University), Hocheol Shin (KAIST), Connor Bolton (University of Michigan), Wenyuan Xu (Zhejiang University), Yongdae Kim (KAIST), and Kevin Fu (University of Michigan)

Session #2: Authentication

Gesture Authentication for Smartphones: Evaluation of Gesture Password Selection Policies .249

Eunyong Cheon (UNIST, Republic of Korea), Yonghwan Shin (UNIST, Republic of Korea), Jun Ho Huh (Samsung Research, Republic of Korea), Hyoungshick Kim (Sungkyunkwan University, Republicof Korea), and Ian Oakley (UNIST, Republic of Korea)

Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication .268

Sanam Ghorbani Lyastani (CISPA Helmholtz Center for Information Security, Germany), Michael Schilling (CISPA Helmholtz Center for Information Security, Germany), Michaela Neumayr (CISPA Helmholtz Center for Information Security, Germany), Michael Backes (CISPA Helmholtz Center for Information Security, Germany), and Sven Bugiel (CISPA Helmholtz Center for Information Security, Germany)

This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs .286

Philipp Markert (Ruhr University Bochum), Daniel V. Bailey (Ruhr University Bochum), Maximilian Golla (Max Planck Institute for Security and Privacy), Markus Dürmuth (Ruhr University Bochum), and Adam J. Aviv (The George Washington University)

Session #2: Machine Learning and Privacy

The Value of Collaboration in Convex Machine Learning with Differential Privacy .304

Nan Wu (Macquarie University), Farhad Farokhi (CSIRO's Data61 / The University of Melbourne), David Smith (CSIRO's Data61 / Australian National University), and Mohamed Ali Kaafar (CSIRO's Data61 / Macquarie University)

Automatically Detecting Bystanders in Photos to Reduce Privacy Risks .318

Rakibul Hasan (Indiana University), David Crandall (Indiana University), Mario Fritz (CISPA Helmholtz Center for Information Security), and Apu Kapadia (Indiana University)

CrypTFlow : Secure TensorFlow Inference .336

Nishant Kumar (Microsoft Research, India), Mayank Rathee (Microsoft Research, India), Nishanth Chandran (Microsoft Research, India), Divya Gupta (Microsoft Research, India), Aseem Rastogi (Microsoft Research, India), and Rahul Sharma (Microsoft Research, India)

Session #3: Differential Privacy

SoK: Differential Privacy as a Causal Property 354
Michael Carl Tschantz (International Computer Science Institute), Shayak Sen (Carnegie Mellon University), and Anupam Datta (Carnegie Mellon University)

Private Resource Allocators and Their Applications 372
Sebastian Angel (University of Pennsylvania), Sampath Kannan (University of Pennsylvania), and Zachary Ratliff (Raytheon BBN Technologies)

Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension 392
Aiping Xiong (Penn State University), Tianhao Wang (Purdue University), Ninghui Li (Purdue University), and Somesh Jha (University of Wisconsin-Madison)

A Programming Framework for Differential Privacy with Accuracy Concentration Bounds 411
Elisabet Lobo-Vesga (Chalmers University of Technology, Sweden), Alejandro Russo (Chalmers University of Technology, Sweden), and Marco Gaboardi (Boston University, USA)

Session #3: Internet of Things

Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products 429
Philipp Morgner (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany), Christoph Mai (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany), Nicole Koschate-Fischer (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany), Felix Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany), and Zinaida Benenson (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany)

Ask the Experts: What Should Be on an IoT Privacy and Security Label? 447
Pardis Emami-Naeini (Carnegie Mellon University), Yuvraj Agarwal (Carnegie Mellon University), Lorrie Faith Cranor (Carnegie Mellon University), and Hanan Hibshi (Carnegie Mellon University)

Burglars' IoT Paradise: Understanding and Mitigating Security Risks of General Messaging Protocols on IoT Clouds 465
Yan Jia (Xidian University, China; University of Chinese Academy of Sciences ,China; Indiana University Bloomington, USA), Luyi Xing (Indiana University Bloomington, USA), Yuhang Mao (Xidian University, China; University of Chinese Academy of Sciences ,China), Dongfang Zhao (Indiana University Bloomington, USA), XiaoFeng Wang (Indiana University Bloomington, USA), Shangru Zhao (Xidian University, China; University of Chinese Academy of Sciences ,China), and Yuqing Zhang (University of Chinese Academy of Sciences ,China; Xidian University, China)

Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses 482
Sunil Manandhar (William & Mary, USA), Kevin Moran (William & Mary, USA), Kaushal Kafle (William & Mary, USA), Ruhao Tang (William & Mary, USA), Denys Poshyvanyk (William & Mary, USA), and Adwait Nadkarni (William & Mary, USA)

Session #3: Wireless Protocols

Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement 500
Patrick Leu (ETH Zurich), Mridula Singh (ETH Zurich), Marc Roeschlin (ETH Zurich), Kenneth G. Paterson (ETH Zurich), and Srdjan Capkun (ETH Zurich)

Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd 517
Mathy Vanhoef (New York University Abu Dhabi) and Eyal Ronen (Tel Aviv University and KU Leuven)

Even Black Cats Cannot Stay Hidden in the Dark: Full-band De-anonymization of Bluetooth Classic Devices 534
Marco Cominelli (CNIT & University of Brescia, Italy), Francesco Gringoli (CNIT & University of Brescia, Italy), Margus Lind (Context Information Security, Scotland, UK), Paul Patras (The University of Edinburgh, Scotland, UK), and Guevara Noubir (Northeastern University, Boston, USA)

BIAS: Bluetooth Impersonation AttackS 549
Daniele Antonioli (École Polytechnique Fédérale de Lausanne (EPFL)), Nils Ole Tippenhauer (CISPA Helmholtz Center for Information Security), and Kasper Rasmussen (University of Oxford)

Session #4: Memory Safety

xMP: Selective Memory Protection for Kernel and User Space 563
Sergej Proskurin (Technical University of Munich, Germany), Marius Momeu (Technical University of Munich, Germany), Seyedhamed Ghavamnia (Stony Brook University, USA), Vasileios P. Kemerlis (Brown University, USA), and Michalis Polychronakis (Stony Brook University, USA)

MarkUs: Drop-in Use-After-Free Prevention for Low-Level Languages 578
Sam Ainsworth (University of Cambridge) and Timothy M. Jones (University of Cambridge)

SEIMI: Efficient and Secure SMAP-Enabled Intra-process Memory Isolation 592

Zhe Wang (Institute of Computing Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Chenggang Wu (Institute of Computing Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Mengyao Xie (Institute of Computing Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Yinqian Zhang (The Ohio State University), Kangjie Lu (University of Minnesota), Xiaofeng Zhang (Institute of Computing Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Yuanming Lai (Institute of Computing Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Yan Kang (Institute of Computing Technology, Chinese Academy of Sciences), and Min Yang (Fudan University)

Cornucopia: Temporal Safety for CHERI Heaps 608

Nathaniel Wesley Filardo (University of Cambridge), Brett F. Gutstein (University of Cambridge), Jonathan Woodruff (University of Cambridge), Sam Ainsworth (University of Cambridge), Lucian Paul-Trifu (University of Cambridge), Brooks Davis (SRI International), Hongyan Xia (University of Cambridge), Edward Tomasz Napierala (University of Cambridge), Alexander Richardson (University of Cambridge), John Baldwin (Ararat River Consulting), David Chisnall (Microsoft Research, Cambridge), Jessica Clarke (University of Cambridge), Khilan Gudka (University of Cambridge), Alexandre Joannou (University of Cambridge), A. Theodore Markettos (University of Cambridge), Alfredo Mazzinghi (University of Cambridge), Robert M. Norton (University of Cambridge), Michael Roe (University of Cambridge), Peter Sewell (University of Cambridge), Stacey Son (University of Cambridge), Timothy M. Jones (University of Cambridge), Simon W. Moore (University of Cambridge), Peter G. Neumann (SRI International), and Robert N. M. Watson (University of Cambridge)

Session #4: Computing and Society

The Many Kinds of Creepware Used for Interpersonal Attacks 626

Kevin A. Roundy (NortonLifeLock Research Group), Paula Barmaimon Mendelberg (Cornell Tech), Nicola Dell (Cornell Tech), Damon McCoy (New York University), Daniel Nissani (Cornell Tech), Thomas Ristenpart (Cornell Tech), and Acar Tamersoy (NortonLifeLock Research Group)

How Not to Prove Your Election Outcome 644

Thomas Haines (Norwegian University of Science and Technology), Sarah Jamie Lewis (Open Privacy Research Society, Canada), Olivier Pereira (UCLouvain ICTEAM), and Vanessa Teague (The University of Melbourne)

A Security Analysis of the Facebook Ad Library 661

Laura Edelson (New York University, USA), Tobias Lauinger (New York University, USA), and Damon McCoy (New York University, USA)

Can Voters Detect Malicious Manipulation of Ballot Marking Devices? 679
Matthew Bernhard (University of Michigan, USA), Allison McDonald (University of Michigan, USA), Henry Meng (University of Michigan, USA), Jensen Hwa (University of Michigan, USA), Nakul Bajaj (The Harker School, USA), Kevin Chang (University of Michigan, USA), and J. Alex Halderman (University of Michigan, USA)

Session #4: Rowhammer

RAMBleed: Reading Bits in Memory without Accessing Them 695
Andrew Kwong (University of Michigan), Daniel Genkin (University of Michigan), Daniel Gruss (Graz University of Technology), and Yuval Yarom (University of Adelaide and Data61)

Are We Susceptible to Rowhammer? An End-to-End Methodology for Cloud Providers 712
Lucian Cojocar (Microsoft Research), Jeremie Kim (ETH Zurich, CMU), Minesh Patel (ETH Zurich), Lillian Tsai (MIT), Stefan Saroiu (Microsoft Research), Alec Wolman (Microsoft Research), and Onur Mutlu (ETH Zurich, CMU)

Leveraging EM Side-Channel Information to Detect Rowhammer Attacks 729
Zhenkai Zhang (Texas Tech University, USA), Zihao Zhan (Vanderbilt University, USA), Daniel Balasubramanian (Vanderbilt University, USA), Bo Li (University of Illinois at Urbana-Champaign, USA), Peter Volgyesi (Vanderbilt University, USA), and Xenofon Koutsoukos (Vanderbilt University, USA)

TRRespass: Exploiting the Many Sides of Target Row Refresh 747
Pietro Frigo (Vrije Universiteit Amsterdam, The Netherlands), Emanuele Vannacci (Vrije Universiteit Amsterdam, The Netherlands), Hasan Hassan (ETH Zürich, Switzerland), Victor van der Veen (Qualcomm Technologies Inc., USA), Onur Mutlu (ETH Zürich, Switzerland), Cristiano Giuffrida (Vrije Universiteit Amsterdam, The Netherlands), Herbert Bos (Vrije Universiteit Amsterdam, The Netherlands), and Kaveh Razavi (Vrije Universiteit Amsterdam, The Netherlands)

Session #5: Web Privacy

AdGraph: A Graph-Based Approach to Ad and Tracker Blocking 763
Umar Iqbal (University of Iowa / Brave Software), Peter Snyder (Brave Software), Shitong Zhu (UC Riverside), Benjamin Livshits (Brave Software / Imperial College London), Zhiyun Qian (UC Riverside), and Zubair Shafiq (University of Iowa)

Browsing Unicity: On the Limits of Anonymizing Web Tracking Data 777
Clemens Deußer (TU Dresden, Germany), Steffen Passmann (INFOnline GmbH, Germany), and Thorsten Strufe (Karlsruhe Institute of Technology (KIT) and Centre for Tactile Internet (TU Dresden), Germany)

Do Cookie Banners Respect My Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework 791

Célestin Matte (Université Côte d'Azur, Inria, France), Nataliia Bielova (Université Côte d'Azur, Inria, France), and Cristiana Santos (University of Minho)

Meddling Middlemen: Empirical Analysis of the Risks of Data-Saving Mobile Browsers 810

Brian Kondracki (Stony Brook University), Assel Aliyeva (Boston University), Manuel Egele (Boston University), Jason Polakis (University of Illinois at Chicago), and Nick Nikiforakis (Stony Brook University)

Session #5: Multiparty Computation

Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers 825

Chun Guo (Université catholique de Louvain), Jonathan Katz (University of Maryland), Xiao Wang (Northwestern University), and Yu Yu (Shanghai Jiao Tong University)

Path Oblivious Heap: Optimal and Practical Oblivious Priority Queue 842

Elaine Shi (Cornell University)

Transparent Polynomial Delegation and Its Applications to Zero Knowledge Proof 859

Jiaheng Zhang (UC Berkeley, USA), Tiancheng Xie (UC Berkeley, USA), Yupeng Zhang (Texas A&M, USA), and Dawn Song (UC Berkeley, USA)

Towards Scalable Threshold Cryptosystems 877

Alin Tomescu (MIT CSAIL), Robert Chen (MIT PRIMES & Lexington High School), Yiming Zheng (MIT PRIMES & Lexington High School), Ittai Abraham (VMware Research), Benny Pinkas (VMware Research & Bar Ilan University), Guy Golan Gueta (VMware Research), and Srinivas Devadas (MIT CSAIL)

Session #5: Blockchain II

A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network 894

Muoi Tran (National University of Singapore), Inho Choi (National University of Singapore), Gi Jun Moon (Korea University), Anh V. Vu (Japan Advanced Institute of Science and Technology), and Min Suk Kang (National University of Singapore)

Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability 910

Philip Daian (Cornell Tech, USA), Steven Goldfeder (Cornell Tech, USA), Tyler Kell (Cornell Tech, USA), Yunqi Li (UIUC, USA), Xueyuan Zhao (Carnegie Mellon University, USA), Iddo Bentov (Cornell Tech, USA), Lorenz Breidenbach (ETH Zurich, Switzerland), and Ari Juels (Cornell Tech, USA)

FlyClient: Super-Light Clients for Cryptocurrencies 928

Benedikt Bünz (Stanford University), Lucianna Kiffer (Northeastern University), Loi Luu (Kyber Network), and Mahdi Zamani (Visa Research)

ZEXE: Enabling Decentralized Private Computation 947
Sean Bowe (Zcash), Alessandro Chiesa (UC Berkeley), Matthew Green (Johns Hopkins University), Ian Miers (Cornell Tech), Pratyush Mishra (UC Berkeley), and Howard Wu (UC Berkeley)

Session #6: Formal Verification

The Last Mile: High-Assurance and High-Speed Cryptographic Implementations 965
José Bacelar Almeida (University of Minho and INESC TEC), Manuel Barbosa (University of Porto (FCUP) and INESC TEC), Gilles Barthe (MPI for Security and Privacy and IMDEA Software), Benjamin Grégoire (Inria), Adrien Koutsos (LSV, CNRS, ENS Paris-Saclay), Vincent Laporte (Inria), Tiago Oliveira (University of Porto (FCUP) and INESC TEC), and Pierre-Yves Strub (Ecole Polytechnique)

EverCrypt: A Fast, Verified, Cross-Platform Cryptographic Provider 983
Jonathan Protzenko (Microsoft Research, USA), Bryan Parno (Carnegie Mellon University, USA), Aymeric Fromherz (Carnegie Mellon University, USA), Chris Hawblitzel (Microsoft Research, USA), Marina Polubelova (Inria, France), Karthikeyan Bhargavan (Inria, France), Benjamin Beurdouche (Inria, France), Joonwon Choi (MIT, USA and Microsoft Research, UK), Antoine Delignat-Lavaud (Microsoft Research, UK), Cédric Fournet (Microsoft Research, UK), Natalia Kulatova (Inria, France), Tahina Ramananandro (Microsoft Research, USA), Aseem Rastogi (Microsoft Research, India), Nikhil Swamy (Microsoft Research, USA), Christoph M. Wintersteiger (Microsoft Research, UK), and Santiago Zanella-Beguelin (Microsoft Research, UK)

Rigorous Engineering for Hardware Security: Formal Modelling and Proof in the CHERI Design and Implementation Process 1003
Kyndylan Nienhuis (University of Cambridge), Alexandre Joannou (University of Cambridge), Thomas Bauereiss (University of Cambridge), Anthony Fox (ARM Limited), Michael Roe (University of Cambridge), Brian Campbell (University of Edinburgh), Matthew Naylor (University of Cambridge), Robert M. Norton (University of Cambridge), Simon W. Moore (University of Cambridge), Peter G. Neumann (SRI International), Ian Stark (University of Edinburgh), Robert N. M. Watson (University of Cambridge), and Peter Sewell (University of Cambridge)

Binsec/Rel: Efficient Relational Symbolic Execution for Constant-Time at Binary-Level 1021
Lesly-Ann Daniel (CEA, List, Université Paris-Saclay, France), Sébastien Bardin (CEA, List, Université Paris-Saclay, France), and Tamara Rezk (INRIA Sophia-Antipolis, INDES Project, France)

Session #6: Android and iOS

An Analysis of Pre-installed Android Software 1039
Julien Gamba (IMDEA Networks Institute, Universidad Carlos III de Madrid), Mohammed Rashed (Universidad Carlos III de Madrid), Abbas Razaghpanah (Stony Brook University), Juan Tapiador (Universidad Carlos III de Madrid), and Narseo Vallina-Rodriguez (IMDEA Networks Institute, ICSI)

Kobold: Evaluating Decentralized Access Control for Remote NSXPC Methods on iOS 1056
Luke Deshotels (North Carolina State University, Samsung Research America), Costin Carabaș (University POLITEHNICA of Bucharest), Jordan Beichler (North Carolina State University), Răzvan Deaconescu (University POLITEHNICA of Bucharest), and William Enck (North Carolina State University)

TextExerciser: Feedback-Driven Text Input Exercising for Android Applications 1071
Yuyu He (Fudan University), Lei Zhang (Fudan University), Zhemin Yang (Fudan University), Yinzhi Cao (Johns Hopkins University), Keke Lian (Fudan University), Shuai Li (Fudan University), Wei Yang (University of Texas at Dallas), Zhibo Zhang (Fudan University), Min Yang (Fudan University), Yuan Zhang (Fudan University), and Haixin Duan (Tsinghua University)

Ex-vivo Dynamic Analysis Framework for Android Device Drivers 1088
Ivan Pustogarov (University of Toronto, Canada), Qian Wu (University of Toronto, Canada), and David Lie (University of Toronto, Canada)

Automatic Uncovering of Hidden Behaviors from Input Validation in Mobile Apps 1106
Qingchuan Zhao (The Ohio State University, USA), Chaoshun Zuo (The Ohio State University, USA), Brendan Dolan-Gavitt (New York University, USA), Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany), and Zhiqiang Lin (The Ohio State University, USA)

Session #6: Attacks and Forensics

PMP: Cost-Effective Forced Execution with Probabilistic Memory Pre-planning 1121
Wei You (Purdue University, USA), Zhuo Zhang (Purdue University, USA), Yonghwi Kwon (University of Virginia, USA), Yousra Aafer (Purdue University, USA), Fei Peng (Purdue University, USA), Yu Shi (Purdue University, USA), Carson Harmon (Purdue University, USA), and Xiangyu Zhang (Purdue University, USA)

Combating Dependence Explosion in Forensic Analysis Using Alternative Tag Propagation Semantics 1139
Md Nahid Hossain (Stony Brook University), Sanaz Sheikhi (Stony Brook University), and R. Sekar (Stony Brook University)

TARDIS: Rolling Back the Clock on CMS-Targeting Cyber Attacks 1156
Ranjita Pai Kasturi (Georgia Institute of Technology, USA), Yiting Sun (Georgia Institute of Technology, USA), Ruian Duan (Georgia Institute of Technology, USA), Omar Alrawi (Georgia Institute of Technology, USA), Ehsan Asdar (Georgia Institute of Technology, USA), Victor Zhu (Georgia Institute of Technology, USA), Yonghwi Kwon (University of Virginia, USA), and Brendan Saltaformaggio (Georgia Institute of Technology, USA)

Tactical Provenance Analysis for Endpoint Detection and Response Systems 1172
Wajih Ul Hassan (University of Illinois at Urbana-Champaign, USA), Adam Bates (University of Illinois at Urbana-Champaign, USA), and Daniel Marino (NortonLifeLock Research Group, USA)

Throwing Darts in the Dark? Detecting Bots with Limited Data Using Neural Data Augmentation 1190

Steve T.K. Jan (University of Illinois at Urbana-Champaign & Virginia Tech, USA), Qingying Hao (University of Illinois at Urbana-Champaign, USA), Tianrui Hu (Virginia Tech, USA), Jiameng Pu (Virginia Tech, USA), Sonal Oswal (Radware, Israel), Gang Wang (University of Illinois at Urbana-Champaign, USA), and Bimal Viswanath (Virginia Tech, USA)

Session #7: Cryptanalysis and Side Channels

JIT Leaks: Inducing Timing Side Channels through Just-In-Time Compilation 1207

Tegan Brennan (University of California, Santa Barbara), Nicolás Rosner (University of California, Santa Barbara), and Tevfik Bultan (University of California, Santa Barbara)

The State of the Uniform: Attacks on Encrypted Databases beyond the Uniform Query Distribution 1223

Evgenios M. Kornaropoulos (UC Berkeley), Charalampos Papamanthou (University of Maryland), and Roberto Tamassia (Brown University)

Pseudorandom Black Swans: Cache Attacks on CTR_DRBG 1241

Shaanan Cohney (University of Pennsylvania, USA), Andrew Kwong (University of Michigan, USA), Shahar Paz (Tel Aviv University, Israel), Daniel Genkin (University of Michigan, USA), Nadia Heninger (University of California, San Diego, USA), Eyal Ronen (Tel Aviv University and COSIC (KU Leuven), Israel and Belgium), and Yuval Yarom (University of Adelaide and Data61, Australia)

Flaw Label: Exploiting IPv6 Flow Label 1259

Jonathan Berger (Bar-Ilan University), Amit Klein (Bar-Ilan University), and Benny Pinkas (Bar-Ilan University)

Session #7: Adversarial Machine Learning

HopSkipJumpAttack: A Query-Efficient Decision-Based Attack 1277

Jianbo Chen (University of California, Berkeley), Michael I. Jordan (University of California, Berkeley), and Martin J. Wainwright (University of California, Berkeley; Voleon Group)

Humpty Dumpty: Controlling Word Meanings via Corpus Modifications 1295

Roei Schuster (Tel Aviv University), Tal Schuster (CSAIL, MIT), Yoav Meri (Cornell Tech), and Vitaly Shmatikov (Cornell Tech)

Privacy Risks of General-Purpose Language Models 1314

Xudong Pan (Fudan University), Mi Zhang (Fudan University), Shouling Ji (Zhejiang University and Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies), and Min Yang (Fudan University)

Intriguing Properties of Adversarial ML Attacks in the Problem Space 1332

Fabio Pierazzi (King's College London), Feargus Pendlebury (King's College London & Royal Holloway, University of London & The Alan Turing Institute), Jacopo Cortellazzi (King's College London), and Lorenzo Cavallaro (King's College London)

Session #7: New Directions and Settings

Influencing Photo Sharing Decisions on Social Media: A Case of Paradoxical Findings 1350
Mary Jean Amon (University of Colorado Boulder), Rakibul Hasan (Indiana University), Kurt Hugenberg (Indiana University), Bennett I. Bertenthal (Indiana University), and Apu Kapadia (Indiana University)

SoK: Cyber Insurance - Technical Challenges and a System Security Roadmap 1367
Savino Dambra (Eurecom), Leyla Bilge (Symantec Research Labs), and Davide Balzarotti (Eurecom)

A Tale of Sea and Sky: On the Security of Maritime VSAT Communications 1384
James Pavur (Oxford University, UK), Daniel Moser (armasuisse, Switzerland), Martin Strohmeier (armasuisse, Switzerland), Vincent Lenders (armasuisse, Switzerland), and Ivan Martinovic (Oxford University, UK)

<<I Know Where You Parked Last Summer>> Automated Reverse Engineering and Privacy Analysis of Modern Cars 1401
Daniel Frassinelli (CISPA Helmholtz Center for Information Security, Saarland Informatics Campus, Germany), Sohyeon Park (CISPA Helmholtz Center for Information Security, Saarland Informatics Campus, Germany), and Stefan Nürnberger (CISPA Helmholtz Center for Information Security, Saarland Informatics Campus, Germany)

Session #8: TEEs and Attestation

SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-Assisted TEE Systems 1416
David Cerdeira (Universidade do Minho), Nuno Santos (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa), Pedro Fonseca (Purdue University), and Sandro Pinto (Universidade do Minho)

OAT: Attesting Operation Integrity of Embedded Devices 1433
Zhichuang Sun (Northeastern University, USA), Bo Feng (Northeastern University, USA), Long Lu (Northeastern University, USA), and Somesh Jha (University of Wisconsin-Madison, USA)

Enabling Rack-scale Confidential Computing Using Heterogeneous Trusted Execution Environment 1450
Jianping Zhu (University of Chinese Academy of Sciences), Rui Hou (University of Chinese Academy of Sciences), XiaoFeng Wang (Indiana University at Bloomington), Wenhao Wang (University of Chinese Academy of Sciences), Jiangfeng Cao (University of Chinese Academy of Sciences), Boyan Zhao (University of Chinese Academy of Sciences), Zhongpu Wang (Institute of Computing Technology, CAS), Yuhui Zhang (University of Chinese Academy of Sciences), Jiameng Ying (University of Chinese Academy of Sciences), Lixin Zhang (Institute of Computing Technology, CAS), and Dan Meng (University of Chinese Academy of Sciences)

Plundervolt: Software-Based Fault Injection Attacks against Intel SGX 1466
Kit Murdock (University of Birmingham), David Oswald (University of Birmingham), Flavio D. Garcia (University of Birmingham), Jo Van Bulck (imec-DistriNet, KU Leuven), Daniel Gruss (Graz University of Technology), and Frank Piessens (imec-DistriNet, KU Leuven)

SEVurity: No Security Without Integrity - Breaking Integrity-Free Memory Encryption with Minimal Assumptions 1483
Luca Wilke (University of Lübeck, Germany), Jan Wichelmann (University of Lübeck, Germany), Mathias Morbitzer (Fraunhofer AISEC, Germany), and Thomas Eisenbarth (University of Lübeck, Germany)

Session #8: Program Analysis

RetroWrite: Statically Instrumenting COTS Binaries for Fuzzing and Sanitization 1497
Sushant Dinesh (Purdue University), Nathan Burow (Purdue University), Dongyan Xu (Purdue University), and Mathias Payer (EPFL)

Unexpected Data Dependency Creation and Chaining: A New Attack to SDN 1512
Feng Xiao (The Pennsylvania State University), Jinquan Zhang (The Pennsylvania State University), Jianwei Huang (Texas A&M University), Guofei Gu (Texas A&M University), Dinghao Wu (The Pennsylvania State University), and Peng Liu (The Pennsylvania State University)

Neutaint: Efficient Dynamic Taint Analysis with Neural Networks 1527
Dongdong She (Columbia University), Yizheng Chen (Columbia University), Abhishek Shah (Columbia University), Baishakhi Ray (Columbia University), and Suman Jana (Columbia University)

KARONTE: Detecting Insecure Multi-binary Interactions in Embedded Firmware 1544
Nilo Redini (University of California, Santa Barbara), Aravind Machiry (University of California, Santa Barbara), Ruoyu Wang (Arizona State University), Chad Spensky (University of California, Santa Barbara), Andrea Continella (University of California, Santa Barbara), Yan Shoshitaishvili (Arizona State University), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)

SPIDER: Enabling Fast Patch Propagation in Related Software Repositories 1562
Aravind Machiry (University of California, Santa Barbara), Nilo Redini (University of California, Santa Barbara), Eric Camellini (Politecnico di Milano), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)

Session #8: Fuzzing

SAVIOR: Towards Bug-Driven Hybrid Testing 1580
Yaohui Chen (Northeastern University), Peng Li (Baidu USA), Jun Xu (Stevens Institute of Technology), Shengjian Guo (Baidu USA), Rundong Zhou (Baidu USA), Yulong Zhang (Baidu USA), Tao Wei (Baidu USA), and Long Lu (Northeastern University)

IJON: Exploring Deep State Spaces via Fuzzing 1597
Cornelius Aschermann (Ruhr University Bochum), Sergej Schumilo (Ruhr University Bochum), Ali Abbasi (Ruhr University Bochum), and Thorsten Holz (Ruhr University Bochum)

Pangolin: Incremental Hybrid Fuzzing with Polyhedral Path Abstraction 1613
Heqing Huang (The Hong Kong University of Science and Technology, China), Peisen Yao (The Hong Kong University of Science and Technology, China), Rongxin Wu (Xiamen University, China), Qingkai Shi (The Hong Kong University of Science and Technology, China), and Charles Zhang (The Hong Kong University of Science and Technology, China)

Fuzzing JavaScript Engines with Aspect-Preserving Mutation 1628
Soyeon Park (Georgia Institute of Technology, USA), Wen Xu (Georgia Institute of Technology, USA), Insu Yun (Georgia Institute of Technology, USA), Daehee Jang (Georgia Institute of Technology, USA), and Taesoo Kim (Georgia Institute of Technology, USA)

Krace: Data Race Fuzzing for Kernel File Systems 1643
Meng Xu (Georgia Institute of Technology), Sanidhya Kashyap (Georgia Institute of Technology), Hanqing Zhao (Georgia Institute of Technology), and Taesoo Kim (Georgia Institute of Technology)

Session #9: Analysis of Smart Contracts

VerX: Safety Verification of Smart Contracts 1661
Anton Permenev (ChainSecurity), Dimitar Dimitrov (ETH Zurich), Petar Tsankov (ChainSecurity), Dana Drachsler-Cohen (ETH Zurich), and Martin Vechev (ETH Zurich)

VeriSmart: A Highly Precise Safety Verifier for Ethereum Smart Contracts 1678
Sunbeom So (Korea University), Myungho Lee (Korea University), Jisu Park (Korea University), Heejo Lee (Korea University), and Hakjoo Oh (Korea University)

Semantic Understanding of Smart Contracts: Executable Operational Semantics of Solidity 1695
Jiao Jiao (Nanyang Technological University, Singapore), Shuanglong Kan (Nanyang Technological University, Singapore), Shang-Wei Lin (Nanyang Technological University, Singapore), David Sanán (Nanyang Technological University, Singapore), Yang Liu (Nanyang Technological University, Singapore), and Jun Sun (Singapore Management University, Singapore)

Session #9: Hardware Security

Transys: Leveraging Common Security Properties across Hardware Designs 1713
Rui Zhang (University of North Carolina at Chapel Hill) and Cynthia Sturton (University of North Carolina at Chapel Hill)

C3APSULe: Cross-FPGA Covert-Channel Attacks through Power Supply Unit Leakage 1728
Ilias Giechaskiel (University of Oxford, United Kingdom), Kasper Bonne Rasmussen (University of Oxford, United Kingdom), and Jakub Szefer (Yale University, USA)

ICAS: An Extensible Framework for Estimating the Susceptibility of IC Layouts to Additive Trojans 1742
Timothy Trippel (University of Michigan), Kang G. Shin (University of Michigan), Kevin B. Bush (MIT Lincoln Laboratory), and Matthew Hicks (Virginia Tech)

Author Index