November 9–13, 2020
Virtual Event, USA

Association for
Computing Machinery

Advancing Computing as a Science & Profession

CCS '20

Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:
ACM SIGSAC

General Chairs:
Jay Ligatti, University of South Florida, USA
Xinming Ou, University of South Florida, USA

Program Chairs:
Jonathan Katz, University of Maryland, USA
Giovanni Vigna, University of California-Santa Barbara, USA

Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery
1601 Broadway, 10th Floor
New York, NY 10019-7434

Copyright © 2020 by the Association for Computing Machinery, Inc. (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from: permissions@acm.org or Fax +1 (212) 869-0481.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through www.copyright.com.

ISBN: 978-1-4503-7089-9

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 30777
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)
+1-212-626-0500 (Global)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org
Hours of Operation: 8:30 am – 4:30 pm ET

Printed in the USA

General Chairs' Welcome

We are happy to welcome you to the 2020 ACM Conference on Computer and Communications Security (CCS). Since 1993, CCS has brought together leading researchers and practitioners to present, observe, and discuss research related to computer security and privacy. CCS is the flagship conference of ACM's Special Interest Group on Security, Audit, and Control (SIGSAC) and has been held annually since 1996. As in the past, this year's program includes outstanding papers presented in the main conference program, as well as during pre- and post-conference workshops.

CCS 2020 is exceptional for being the first CCS gathering hosted entirely online. Planning for CCS 2020 began well over a year in advance and targeted Orlando, Florida, USA as the location for a face-to-face gathering. However, due to the global COVID-19 pandemic, and the resulting impossibility of convening over a thousand attendees in a single venue, in mid-2020 the conference organizers began creating contingency plans for hosting CCS online, as a virtual conference. Moving CCS 2020 online required rethinking many conference details, including hosting technologies, presentation schedules, registration fees, and sponsorship benefits. The organizing committee hopes that our decisions enable everyone to experience CCS 2020 positively, with as many benefits as possible being retained from traditional face-to-face conferences, while providing some additional benefits such as reduced travel and fees.

CCS is only possible through the hard work of the research community and many volunteers. We wish to thank the authors who submitted papers for consideration and the program committee who arranged an outstanding program. We are deeply indebted to the extensive CCS 2020 organizing committee, including the program chairs, web chair, treasurer, publication chairs, sponsorship chairs, registration chairs, workshop chair, publicity chairs, student conference grant chairs, poster/demo chair, and virtual conference task force. The conference steering committee, ACM, SIGSAC, and student volunteers have also provided valuable organizational, technical, and administrative support. We further thank the conference sponsors for their generous financial support.

We hope that you have a positive experience at ACM CCS 2020 and are able to learn about and discuss state-of-the-art research in computer and communications security while using the virtual conference platform.

Jay Ligatti
University of South Florida

Xinming Ou
University of South Florida

Program Chairs’ Welcome

These are interesting times.

This year, due to the COVID-19 pandemic, we are holding a virtual conference. Thanks to the heroic efforts of the General Chairs, however, we are using various technologies to foster interaction among attendees, so that our community can continue to hold discussions and exchange ideas even when we cannot be physically co-located.

Selecting papers is always a challenging task, but it was made even more challenging this year due to the additional demands and general stress put on authors, program-committee members, area chairs, and the program chairs themselves. Nevertheless, they all rose to the task and we were able to follow a process similar to the one used for this conference last year. As in 2019, there were two submission deadlines this year (in January and May), each with a roughly 2.5-month review cycle. Due to the large number of papers submitted, and also to give authors the opportunity to submit their papers elsewhere, some papers were rejected early in the process, for the most part only following two high-confidence, negative reviews. For the remaining papers, authors were given the opportunity to provide a rebuttal addressing specific concerns of the reviewers. By the end of each cycle, each submitted paper was marked for acceptance, conditional acceptance (shepherding), rejection, or revision. Papers in the last category were allowed to be resubmitted for another round of review, with the intention that they would be accepted if specific changes recommended by the reviewers (in some cases requiring extensive work) were made. All submissions were reviewed by a program committee of 157 security and privacy experts from around the world, along with many expert subreviewers from outside the committee, with the vast majority of papers (not including papers that were rejected early) receiving 4-5 reviews. The program chairs were assisted by 9 area chairs who are recognized experts in their respective subfields. The area chairs were also involved in selecting the award papers.

The January cycle received 235 submissions, with 26 accepted (including those accepted with shepherding). An additional 14 papers were chosen for revision, with 13 of those eventually being accepted as well. Of the papers that were rejected, 113 were rejected early. A total of 480 papers were submitted to the May cycle, with 52 papers accepted (some with shepherding), and 35 papers chosen to be revised. From the latter group, 30 papers were eventually accepted. Of the rejected papers, 171 were rejected early. Altogether, 121 out of 715 submissions were accepted, for an acceptance rate of 17%.

The accepted papers cover a wide range of topics in security, including machine learning, network security, formal methods, IoT/CPS security, applied cryptography, binary analysis, privacy, and hardware security. This diversity showcases the breadth of research in the field.

We thank the area chairs, PC members, and external reviewers for their contributions to the conference and for their dedication to reviewing under challenging circumstances. We are also extremely grateful to the General Chairs, Jay Ligatti and Xinming Ou, for organizing the virtual conference, and to the Publication Chairs, Mehran Mozaffari Kermani and Ryan Gerdes, for working with the publisher to produce the proceedings. We also thank all the authors for submitting their work to ACM CCCS this year.

We hope you enjoy the conference!

Jonathan Katz
University of Maryland

Giovanni Vigna
University of California, Santa Barbara

Table of Contents

CCS 2020 Conference Organization xvii

ACM CCS 2020 Sponsor & Supporters xxiii

Keynote Talk I

- **Machine Learning and Security: The GoodThe Badand The Ugly** 1
  Wenke Lee *(Georgia Institute of Technology)*

Session 1A: Anonymous Routing and Censorship

- **Bypassing Tor Exit Blocking with Exit Bridge Onion Services** 3
  Zhao Zhang, Wenchao Zhou, Micah Sherr *(Georgetown University)*
- **CLAPS: Client-Location-Aware Path Selection in Tor** 17
  Florentin Rochet *(UCLouvain)*, Ryan Wails, Aaron Johnson *(U.S. Naval Research Laboratory)*,
  Prateek Mittal *(Princeton University)*, Olivier Pereira *(UCLouvain)*
- **Poking a Hole in the Wall: Efficient Censorship-Resistant Internet Communications by Parasitizing on WebRTC** 35
  Diogo Barradas, Nuno Santos, Luís Rodrigues, Vítor Nunes
  (INESC-IDInstituto Superior Técnico, Universidade de Lisboa)
- **Censored Planet: An Internet-wideLongitudinal Censorship Observatory** 49
  Ram Sundara Raman, Prerana Shenoy *(University of Michigan)*, Katharina Kohls *(Ruhr University Bochum)*,
  Roya Ensafi *(University of Michigan)*

Session 1B: Attacking and Defending ML Systems

- **Gotta Catch?Em All: Using Honeypots to Catch Adversarial Attacks on Neural Networks** 67
  Shawn Shan, Emily Wenger, Bolun Wang *(University of Chicago)*,
  Bo Li *(University of Illinois at Urbana-Champaign)*, Haitao Zheng, Ben Y. Zhao *(University of Chicago)*
- **A Tale of Evil Twins: Adversarial Inputs versus Poisoned Models** 85
  Ren Pang, Hua Shen, Xinyang Zhang *(Pennsylvania State University)*, Shouling Ji *(Zhejiang University)*,
  Yevgeniy Vorobeychik *(Washington University in St. Louis)*, Xiapu Luo *(Hong Kong Polytechnic University)*,
  Alex Liu *(Ant Financia)*, Ting Wang *(Pennsylvania State University)*
- **DeepDyve: Dynamic Verification for Deep Neural Networks** 101
  Yu Li *(The Chinese University of Hong Kong)*,
  Min Li, Bo Luo, Ye Tian, Qiang Xu *(The Chinese University of Hong Kong)*
- **Composite Backdoor Attack for Deep Neural Network by Mixing Existing Benign Features** 113
  Junyu Lin, Lei Xu *(Nanjing University)*, Yingqi Liu, Xiangyu Zhang *(Purdue University)*

Session 1C: Binary Analysis/Policy and Access Control

- **Devil is Virtual: Reversing Virtual Inheritance in C++ Binaries** 133
  Rukayat Ayomide Erinfolami, Aravind Prakash *(Binghamton University)*
- **PatchScope: Memory Object Centric Patch Diffing** 149
  Lei Zhao, Yuncong Zhu *(Wuhan University)*, Jiang Ming *(University of Texas at Arlington)*,
  Yichen Zhang *(Wuhan University)*, Haotian Zhang *(University of Texas at Arlington)*,
  Heng Yin *(University of California, Riverside)*
- **FirmXRay: Detecting Bluetooth Link Layer Vulnerabilities From Bare-Metal Firmware** 167
  Haohuang Wen, Zhiqiang Lin, Yinqian Zhang *(Ohio State University)*
- **Privaros: A Framework for Privacy-Compliant Delivery Drones** 181
  Rakesh Rajan Beck, Abhishek Vijeev, Vinod Ganapathy *(Indian Institute of Science)*

Session 1D: Applied Cryptography and Cryptanalysis

- **A PerformantMisuse-Resistant API for Primality Testing** 195
  Jake Massimo *(Royal Holloway, University of London)*, Kenneth G. Paterson *(ETH Zurich)*

- **ProMACs: Progressive and Resynchronizing MACs for Continuous Efficient Authentication of Message Streams** 211
  Frederik Armknecht *(University of Mannheim)* Paul Walther *(TU Dresden)*,
  Gene Tsudik *(University of California, Irvine)*, Martin Beck *(TU Dresden)*,
  Thorsten Strufe *(KIT and CeTI TU Dresden)*

- ***LadderLeak:* Breaking ECDSA with Less than One Bit of Nonce Leakage** 225
  Diego F. Aranha *(Aarhus University)*, Felipe Rodrigues Novaes *(University of Campinas)*,
  Akira Takahashi *(Aarhus University)*, Mehdi Tibouchi *(NTT Corporation)*,
  Yuval Yarom *(University of Adelaide & Data61)*

- **Security of Streaming Encryption in Google's Tink Library** 243
  Viet Tung Hoang *(Florida State University)*, Yaobin Shen *(Shanghai Jiao Tong Univeristy)*

Session 1E: Cyberphysical Systems

- **Cyber-Physical Inconsistency Vulnerability Identification for Safety Checks in Robotic Vehicles** 263
  Hongjun Choi, Sayali Kate *(Purdue University)*, Yousra Aafer *(University of Waterloo)*,
  Xiangyu Zhang, Dongyan Xu *(Purdue University)*

- **HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems** 279
  Efrén López-Morales *(Arizona State University)*, Carlos Rubio-Medrano *(Texas A&M University - Corpus Christi)*,
  Adam Doupé, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, Gail-Joon Ahn *(Arizona State University)*

- **Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks** 293
  Ben Nassi *(Ben-Gurion University of the Negev)*,
  Yisroel Mirsky *(Ben-Gurion University of the Negev & Georgia Institute of Technology)*,
  Dudi Nassi, Raz Ben-Netanel *(Ben-Gurion University of the Negev)*, Oleg Drokin *(Independent Researcher)*,
  Yuval Elovici *(Ben Gurion University of the Negev)*

- **T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices** 309
  Xiaopeng Li, Qiang Zeng, Lannan Luo *(University of South Carolina)*, Tongbo Luo *(JD.com)*

Session 2A: ML and Information Leakage

- **CrypTFlow2: Practical 2-Party Secure Inference** 325
  Deevashwer Rathee, Mayank Rathee, Nishant Kumar, Nishanth Chandran, Divya Gupta, Aseem Rastogi, Rahul Sharma *(Microsoft Research)*

- **GAN-Leaks: A Taxonomy of Membership Inference Attacks against Generative Models** 343
  Dingfan Chen *(CISPA Helmholtz Center for Information Security)*,
  Ning Yu *(University of Maryland & Max Planck Institute for Informatics)*,
  Yang Zhang, Mario Fritz *(CISPA Helmholtz Center for Information Security)*

- **Analyzing Information Leakage of Updates to Natural Language Models** 363
  Santiago Zanella-Béguelin, Lukas Wutschitz, Shruti Tople, Victor Rühle, Andrew Paverd *(Microsoft)*,
  Olga Ohrimenko *(University of Melbourne)*, Boris Köpf, Marc Brockschmidt *(Microsoft)*

- **Information Leakage in Embedding Models** 377
  Congzheng Song *(Cornell University & Google Brain)*, Ananth Raghunathan *(Facebook & Google Brain)*

Session 2B: Applied Cryptography

- **PPE Circuits: Formal Definition to Software Automation** 391
  Susan Hohenberger *(Johns Hopkins University)*, Satyanarayana Vusirikala *(University of Texas at Austin)*,
  Brent Waters *(University of Texas at Austin & NTT Research)*

- **Threshold Password-Hardened Encryption Services** 409
  Julian Brost, Christoph Egger, Russell W. F. Lai, Fritz Schmid,
  Dominique Schröder *(Friedrich-Alexander University Erlangen-Nuremberg)*,
  Markus Zoppelt *(Nuremberg Institute of Technology)*
- **Minimal Symmetric PAKE and 1-out-of-*N* OT from Programmable-Once Public Functions** ..425
  Ian McQuoid, Mike Rosulek, Lawrence Roy *(Oregon State University)*
- **Full Database Reconstruction in Two Dimensions**....................443
  Francesca Falzon, Evangelia Anna Markatou, Akshima, David Cash, Adam Rivkin,
  Jesse Stern *(University of Chicago)*, Roberto Tamassia *(Brown University)*

Session 2C: Browser Security

- **Slimium: Debloating the Chromium Browser with Feature Subsetting** 461
  Chenxiong Qian, Hyungjoon Koo, ChangSeok Oh, Taesoo Kim, Wenke Lee *(Georgia Institute of Technology)*
- **You've Changed: Detecting Malicious Browser Extensions through their Update Deltas**.........477
  Nikolaos Pantelaios *(North Carolina State University)*, Nick Nikiforakis *(Stony Brook University)*,
  Alexandros Kapravelos *(North Carolina State University)*
- **PMForce: Systematically Analyzing postMessage Handlers at Scale**....................493
  Marius Steffens, Ben Stock *(CISPA Helmholtz Center for Information Security)*
- **Fill in the Blanks: Empirical Analysis of the Privacy Threats of Browser Form Autofill** 507
  Xu Lin, Panagiotis Ilia, Jason Polakis *(University of Illinois at Chicago)*

Session 2D: Mobile Security

- **Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China** 521
  Yiming Zhang, Baojun Liu, Chaoyi Lu *(Beijing National Research Center for Information Science and Technology & Tsinghua University)*,
  Zhou Li *(University of California, Irvine)*,
  Haixin Duan *(Beijing National Research Center for Information Science and Technology, Tsinghua University & QI-ANXIN Group)*,
  Shuang Hao *(University of Texas at Dallas)*,
  Mingxuan Liu, Ying Liu *(Beijing National Research Center for Information Science and Technology & Tsinghua University)*,
  Dong Wang, Qiang Li *(360 Mobile Safe)*
- **VAHunt: Warding Off New Repackaged Android Malware in App-Virtualization's Clothing**....................535
  Luman Shi *(Wuhan University)*, Jiang Ming *(University of Texas at Arlington)*,
  Jianming Fu, Guojun Peng *(Wuhan University)*, Dongpeng Xu *(University of New Hampshire)*,
  Kun Gao, Xuanchen Pan *(Wuhan Antiy Information Technology)*
- **Deploying Android Security Updates: an Extensive Study Involving ManufacturersCarriersand End Users** 551
  Kailani R. Jones *(University of Kansas)*, Ting-Fang Yen, Sathya Chandran Sundaramurthy *(DataVisor, Inc.)*,
  Alexandru G. Bardas *(University of Kansas)*
- **Demystifying Resource Management Risks in Emerging Mobile App-in-App Ecosystems**......569
  Haoran Lu, Luyi Xing, Yue Xiao, Yifan Zhang, Xiaojing Liao, XiaoFeng Wang, Xueqiang Wang
  (Indiana University Bloomington)

Session 2E: Smart Contracts and Cryptocurrencies

- **ACE: Asynchronous and Concurrent Execution of Complex Smart Contracts**....................587
  Karl Wüst, Sinisa Matetic, Silvan Egli, Kari Kostiainen, Srdjan Capkun *(ETH Zurich)*

- **BDoS: Blockchain Denial-of-Service** 601
  Michael Mirkin *(Technion and IC3)*, Yan Ji *(Cornell Tech and IC3)*,
  Jonathan Pang, Ariah Klages-Mundt *(Cornell University)*, Ittay Eyal *(Technion and IC3)*,
  Ari Juels *(Cornell Tech and IC3)*
- ***eThor*: Practical and Provably Sound Static Analysis of Ethereum Smart Contracts** 621
  Clara Schneidewind, Ilya Grishchenko, Markus Scherer, Matteo Maffei *(TU Wien)*
- **WI is Almost Enough: Contingent Payment All Over Again** 641
  Ky Nguyen *(École Normale Superieure, CNRS & PSL University)*,
  Miguel Ambrona, Masayuki Abe *(NTT Secure Platform Laboratories)*

Session 3A: Privacy

- **Private Summation in the Multi-Message Shuffle Model** 657
  Borja Balle *(Unaffiliated)*, James Bell *(The Alan Turing Institute)*, Adrià Gascón *(Google)*,
  Kobbi Nissim *(Georgetown University)*
- **R^{2}DP: A Universal and Automated Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions** 677
  Meisam Mohammady *(Concordia University)*, Shangyu Xie, Yuan Hong *(Illinois Institute of Technology)*,
  Mengyuan Zhang *(Ericsson Security Research)*, Lingyu Wang *(Concordia University)*,
  Makan Pourzandi *(Ericsson Security Research)*, Mourad Debbabi *(Concordia University)*
- **Estimating g-Leakage via Machine Learning** 697
  Marco Romanelli *(Inria & École Polytechnique & IPP & Università di Siena)*,
  Konstantinos Chatzikokolakis *(University of Athens)*, Catuscia Palamidessi *(Inria & École Polytechnique & IPP)*,
  Pablo Piantanida *(CentraleSupelec & CNRS & Université Paris Saclay)*
- **Implementing the Exponential Mechanism with Base-2 Differential Privacy** 717
  Christina Ilvento *(Harvard John A. Paulson School of Engineering and Applied Sciences)*

Session 3B: Malware

- **Examining Mirai's Battle over the Internet of Things** 743
  Harm Griffioen, Christian Doerr *(Hasso Plattner Institute for Digital Engineering University of Potsdam)*
- **Enhancing State-of-the-art Classifiers with API Semantics to Detect Evolved Android Malware** 757
  Xiaohan Zhang, Yuan Zhang, Ming Zhong, Daizong Ding *(Fudan University)*,
  Yinzhi Cao *(Johns Hopkins University)*, Yukun Zhang, Mi Zhang, Min Yang *(Fudan University)*
- **Towards Attribution in Mobile Markets: Identifying Developer Account Polymorphism** 771
  Silvia Sebastian *(IMDEA Software Institute & Universidad Politécnica de Madrid)*, Juan Caballero *(IMDEA Software Institute)*
- **Mnemosyne: An Effective and Efficient Postmortem Watering Hole Attack Investigation System** 787
  Joey Allen, Zheng Yang, Matthew Landen, Raghav Bhat, Harsh Grover,
  Andrew Chang *(Georgia Institute of Technology)*, Yang Ji *(Palo Alto Networks)*,
  Roberto Perdisci *(Georgia Institute of Technology & University of Georgia)*,
  Wenke Lee *(Georgia Institute of Technology)*

Session 3C: Consensus

- **Dumbo: Faster Asynchronous BFT Protocols** 803
  Bingyong Guo *(IS, CAS, UCAS & JDD-NJIT-ISCAS Joint Blockchain Lab)*, Zhenliang Lu, Qiang Tang *(New Jersey Institute of Technology & JDD-NJIT-ISCAS Joint Blockchain Lab)*, Jing Xu, Zhenfeng Zhang *(Institute of Software, Chinese Academy of Sciences & JDD-NJIT-ISCAS Joint Blockchain Lab)*
- **Tight Consistency Bounds for Bitcoin** 819
  Peter Gaži *(IOHK)*, Aggelos Kiayias, Alexander Russell *(University of Connecticut & IOHK)*

- **On the Optimality of Optimistic Responsiveness** 839
  Nibesh Shrestha *(Rochester Institute of Technology)*, Ittai Abraham *(VMware Research)*,
  Ling Ren *(University of Illinois at Urbana-Champaign)*, Kartik Nayak *(Duke University)*

- **Everything is a Race and Nakamoto Always Wins** 859
  Amir Dembo *(Stanford University)*, Sreeram Kannan *(University of Washington)*,
  Ertem Nusret Tas, David Tse *(Stanford University)*,
  Pramod Viswanath, Xuechao Wang *(University of Illinois at Urbana-Champaign)*,
  Ofer Zeitouni *(Weizmann Institute of Science)*

Session 3D: Formal Methods

- **Security Analysis and Implementation of Relay-Resistant Contactless Payments** 879
  Ioana Boureanu *(University of Surrey)*, Tom Chothia *(University of Birmingham)*,
  Alexandre Debant, Stéphanie Delaune *(University of Rennes, CNRS, IRISA)*

- **HACLxN: Verified Generic SIMD Crypto (for all your favourite platforms)** 899
  Marina Polubelova, Karthikeyan Bhargavan *(Inria Paris)*, Jonathan Protzenko *(Microsoft Research)*,
  Benjamin Beurdouche *(Inria Paris & Mozilla)*, Aymeric Fromherz *(Carnegie Mellon University)*,
  Natalia Kulatova *(Inria Paris)*, Santiago Zanella-Béguelin *(Microsoft Research)*

- **CheckDP: An Automated and Integrated Approach for Proving Differential Privacy or Finding Precise Counterexamples** 919
  Yuxin Wang, Zeyu Ding, Daniel Kifer, Danfeng Zhang *(The Pennsylvania State University)*

- **Asynchronous Remote Key Generation: An Analysis of Yubico's Proposal for W3C WebAuthn** 939
  Nick Frymann, Daniel Gardham *(University of Surrey)*, Franziskus Kiefer *(Wire Swiss GmbH)*,
  Emil Lundberg *(Yubico AB)*, Mark Manulis *(University of Surrey)*, Dain Nilsson *(Yubico AB)*

Session 3E: Fuzzing/Trusted Execution Environments

- **SQUIRREL: Testing Database Management Systems with Language Validity and Coverage Feedback** 955
  Rui Zhong *(The Pennsylvania State University)*, Yongheng Chen, Hong Hu *(Georgia Institute of Technology)*,
  Hangfan Zhang *(The Pennsylvania State University)*, Wenke Lee *(Georgia Institute of Technology)*,
  Dinghao Wu *(The Pennsylvania State University)*

- **FREEDOM: Engineering a State-of-the-Art DOM Fuzzer** 971
  Wen Xu, Soyeon Park, Taesoo Kim *(Georgia Institute of Technology)*

- **BlackMirror: Preventing Wallhacks in 3D Online FPS Games** 987
  Seonghyun Park *(Seoul National University)*, Adil Ahmad *(Purdue University)*,
  Byoungyoung Lee *(Seoul National University)*

- **Cache-in-the-Middle (CITM) Attacks : Manipulating Sensitive Data in Isolated Execution Environments** 1001
  Jie Wang *(Institute of Information Engineering, CAS & George Mason University)*,
  Kun Sun *(George Mason University)*,
  Lingguang Lei *(Institute of Information Engineering, CAS & University of Chinese Academy of Sciences)*,
  Shengye Wan *(College of William and Mary & George Mason University)*,
  Yuewu Wang *(Institute of Information Engineering, CAS & University of Chinese Academy of Sciences)*,
  Jiwu Jing *(University of Chinese Academy of Sciences)*

Session 4A: Post-Quantum Cryptography

- **Deterministic Wallets in a Quantum World** 1017
  Nabil Alkeilani Alkadri, Poulami Das, Andreas Erwig, Sebastian Faust, Juliane Krämer, Siavash Riahi,
  Patrick Struck *(Technische Universität Darmstadt)*

- **SNI-in-the-head: Protecting MPC-in-the-head Protocols against Side-channel Analysis** 1033
  Okan Seker, Sebastian Berndt, Luca Wilke, Thomas Eisenbarth *(University of Lübeck)*

- **Practical Lattice-Based Zero-Knowledge Proofs for Integer Relations** 1051
  Vadim Lyubashevsky *(IBM Research - Zurich)*,
  Ngoc Khanh Nguyen, Gregor Seiler *(IBM Research - Zurich and ETH Zurich)*
- **QuantumHammer: A Practical Hybrid Attack on the LUOV Signature Scheme** 1071
  Koksal Mus, Saad Islam, Berk Sunar *(Worcester Polytechnic Institute)*

Session 4B: Physical Attacks

- **TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-signal SoCs** 1085
  Jieun Choi *(Korea Advanced Institute of Science and Technology)*,
  Hae-Yong Yang *(The Affiliated Institute of ETRI)*,
  Dong-Ho Cho *(Korea Advanced Institute of Science and Technology)*
- **When the Differences in Frequency Domain are Compensated: Understanding and Defeating Modulated Replay Attacks on Automatic Speech Recognition** 1103
  Shu Wang *(George Mason University)*, Jiahao Cao *(George Mason University & Tsinghua University)*,
  Xu He, Kun Sun *(George Mason University)*, Qi Li *(Tsinghua University)*
- **AdvPulse: Universal, Synchronization-free, and Targeted Audio Adversarial Attacks via Subsecond Perturbations** 1121
  Zhuohang Li, Yi Wu, Jian Liu *(University of Tennessee, Knoxville)*, Yingying Chen, Bo Yuan *(Rutgers University)*
- **Harnessing the Ambient Radio Frequency Noise for Wearable Device Pairing** 1135
  Wenqiang Jin, Ming Li, Srinivasan Murali *(The University of Texas at Arlington)*,
  Linke Guo *(Clemson University)*

Session 4C: Kernel Security

- **PDiff: Semantic-based Patch Presence Testing for Downstream Kernels** 1149
  Zheyue Jiang, Yuan Zhang *(Fudan University)*, Jun Xu *(Stevens Institute of Technology)*,
  Qi Wen, Zhenghe Wang, Xiaohan Zhang *(Fudan University)*, Xinyu Xing *(The Pennsylvania State University)*,
  Min Yang, Zhemin Yang *(Fudan University)*
- **A Systematic Study of Elastic Objects in Kernel Exploitation** 1165
  Yueqi Chen, Zhenpeng Lin, Xinyu Xing *(The Pennsylvania State University)*
- ***iDEA*: Static Analysis on the Security of Apple Kernel Drivers** 1185
  Xiaolong Bai *(Orion Security Lab, Alibaba Group)*, Luyi Xing *(Indiana University Bloomington)*,
  Min Zheng, Fuping Qu *(Orion Security Lab, Alibaba Group)*
- **Exaggerated Error Handling Hurts! An In-Depth Study and Context-Aware Detection** 1203
  Aditya Pakki, Kangjie Lu *(University of MinnesotaTwin Cities)*

Session 4D: Distributed Protocols

- **LEAF: A Faster Secure Search Algorithm via Localization, Extraction, and Reconstruction** .. 1219
  Rui Wen *(CISPA Helmholtz Center for Information Security)*, Yu Yu *(Shanghai Jiao Tong University)*,
  Xiang Xie *(PlatON)*, Yang Zhang *(CISPA Helmholtz Center for Information Security)*
- **Blinder -- ScalableRobust Anonymous Committed Broadcast** 1233
  Ittai Abraham *(VMware Research)*, Benny Pinkas *(Bar Ilan University)*, Avishay Yanai *(VMware Research)*
- **Secure Single-Server Aggregation with (Poly)Logarithmic Overhead** 1253
  James Henry Bell *(The Alan Turing Institute)*,
  Kallista A. Bonawitz, Adrià Gascón, Tancrède Lepoint, Mariana Raykova *(Google)*
- **Fast Database Joins and PSI for Secret Shared Data** 1271
  Payman Mohassel *(Facebook)*, Peter Rindal *(Visa Research)*, Mike Rosulek *(Oregon State University)*

Session 4E: Network Security

- **The Boon and Bane of Cross-Signing: Shedding Light on a Common Practice in Public Key Infrastructures** 1289
  Jens Hiller *(RWTH Aachen University)*, Johanna Amann *(ICSI, Corelight & LBNL)*,
  Oliver Hohlfeld *(Brandenburg University of Technology)*
- **Zombie Awakening: Stealthy Hijacking of Active Domains through DNS Hosting Referral** 1307
  Eihal Alowaisheq *(Indiana University & King Saud University)*, Siyuan Tang *(Indiana University)*,
  Zhihao Wang *(Institute of Information EngineeringChinese Academy of Sciences)*,
  Fatemah Alharbi *(Taibah University)*, Xiaojing Liao, XiaoFeng Wang *(Indiana University)*
- **Off-Path TCP Exploits of the Mixed IPID Assignment** 1323
  Xuewei Feng, Chuanpu Fu, Qi Li *(Tsinghua University)*, Kun Sun *(George Mason University)*,
  Ke Xu *(Tsinghua University & Peng Cheng Laboratory)*
- **DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels** 1337
  Keyu Man, Zhiyun Qian, Zhongjie Wang *(University of California, Riverside)*,
  Xiaofeng Zheng *(Qi-AnXin Group & Tsinghua University)*, Youjun Huang *(Tsinghua University)*,
  Haixin Duan *(Tsinghua University & Qi-AnXin Group)*

Session 5A: User Authentication

- **Game-Set-MATCH: Using Mobile Devices for Seamless External-Facing Biometric Matching** 1351
  Shashank Agrawal *(Western Digital)*,
  Saikrishna Badrinarayanan, Pratyay Mukherjee, Peter Rindal *(Visa Research)*
- **Usage Patterns of Privacy-Enhancing Technologies** 1371
  Kovila P.L. Coopamootoo *(Newcastle University)*
- **Text Captcha Is Dead? A Large Scale Deployment and Empirical Study** 1391
  Chenghui Shi, Shouling Ji, Qianjun Liu *(Zhejiang University)*, Changchang Liu *(IBM Research)*,
  Yuefeng Chen, Yuan He *(Alibaba Group)*, Zhe Liu *(Nanjing University of Aeronautics and Astronautics)*,
  Raheem Beyah *(Georgia Institute of Technology)*, Ting Wang *(Penn State)*
- **Practical Recommendations for StrongerMore Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements** 1407
  Joshua Tan, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor *(Carnegie Mellon University)*

Session 5B: Secure Messaging and Key Exchange

- **Oracle Simulation: A Technique for Protocol Composition with Long Term Shared Secrets** 1427
  Hubert Comon, Charlie Jacomme *(LSVCNRS & ENS Paris-Saclay & Inria & Université Paris-Saclay)*,
  Guillaume Scerri *(Université Versailles Saint-Quentin & Inria)*
- **The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption** 1445
  Melissa Chase *(Microsoft Research)*, Trevor Perrin *(Signal Technology Foundation)*,
  Greg Zaverucha *(Microsoft Research)*
- **Post-Quantum TLS Without Handshake Signatures** 1461
  Peter Schwabe *(Max Planck Institute for Security and Privacy & Radboud University)*,
  Douglas Stebila, Thom Wiggers *(Radboud University)*
- **Clone Detection in Secure Messaging: Improving Post-Compromise Security in Practice** 1481
  Cas Cremers, Jaiden Fairoze, Benjamin Kiesl, Aurora Naska *(CISPA Helmholtz Center for Information Security)*

Session 5C: Forensics

- **A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet** 1497
  Brian N. Levine, Marc Liberatore, Brian Lynn *(University of Massachusetts, Amherst)*,
  Matthew Wright *(Rochester Institute of Technology)*
- **A Qualitative Study of Dependency Management and Its Security Implications** 1513
  Ivan Pashchenko, Duc-Ly Vu *(University of Trento)*,
  Fabio Massacci *(University of Trento & Vrije Universiteit Amsterdam)*
- **Forensic Analysis in Access Control: Foundations and a Case-Study from Practice** 1533
  Nahid Juma, Xiaowei Huang, Mahesh Tripunitara *(University of Waterloo)*
- **Logging to the Danger Zone: Race Condition Attacks and Defenses on System Audit Frameworks** 1551
  Riccardo Paccagnella, Kevin Liao *(University of Illinois at Urbana-Champaign)*, Dave Tian *(Purdue University)*,
  Adam Bates *(University of Illinois at Urbana-Champaign)*

Session 5D: Secure Computation

- **MP-SPDZ: A Versatile Framework for Multi-Party Computation**.. 1575
  Marcel Keller *(CSIRO's Data61)*
- **Is the Classical GMW Paradigm Practical? The Case of Non-Interactive Actively Secure 2PC**.................. 1591
  Jackson Abascal, Mohammad Hossein Faghihi Sereshgi *(University of Rochester)*,
  Carmit Hazay *(Bar-Ilan University)*, Yuval Ishai *(Technion)*,
  Muthuramakrishnan Venkitasubramaniam *(University of Rochester)*
- **Ferret: Fast Extension for Correlated OT with Small Communication** 1607
  Kang Yang *(State Key Laboratory of Cryptology)*, Chenkai Weng *(Northwestern University)*,
  Xiao Lan *(Sichuan University)*, Jiang Zhang *(State Key Laboratory of Cryptology)*,
  Xiao Wang *(Northwestern University)*
- **More Efficient MPC from Improved Triple Generation and Authenticated Garbling** 1627
  Kang Yang *(State Key Laboratory of Cryptology)*, Xiao Wang *(Northwestern University)*,
  Jiang Zhang *(State Key Laboratory of Cryptology)*

Session 5E: Infrastructure Security

- **Mitigation of Attacks on Email End-to-End Encryption** 1647
  Jörg Schwenk, Marcus Brinkmann *(Ruhr University Bochum)*,
  Damian Poddebniak *(Münster University of Applied Sciences)*, Jens Müller *(Ruhr University Bochum)*,
  Juraj Somorovsky *(Paderborn University)*, Sebastian Schinzel *(Münster University of Applied Sciences)*
- **Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale** 1665
  Michele Campobasso, Luca Allodi *(Eindhoven University of Technology)*
- **VisualPhishNet: Zero-Day Phishing Website Detection by Visual Similarity**.............................. 1681
  Sahar Abdelnabi, Katharina Krombholz, Mario Fritz *(CISPA Helmholtz Center for Information Security)*
- **Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certification in Voice Personal Assistant Platforms** 1699
  Long Cheng, Christin Wilson, Song Liao, Jeffrey Young, Daniel Dong, Hongxin Hu *(Clemson University)*

Session 6A: Signatures

- **MuSig-DN: Schnorr Multi-Signatures with Verifiably Deterministic Nonces** 1717
  Jonas Nick, Tim Ruffing *(Blockstream)*, Yannick Seurin *(ANSSI)*, Pieter Wuille *(Blockstream)*
- **Verifiable Timed Signatures Made Practical** 1733
  Sri Aravinda Krishnan Thyagarajan *(Friedrich Alexander Universität Erlangen-Nürnberg)*,
  Adithya Bhat *(Purdue University)*, Giulio Malavolta *(University of California, Berkeley & CMU)*,
  Nico Döttling *(CISPA Helmholtz Center for Information Security)*, Aniket Kate *(Purdue University)*,
  Dominique Schröder *(Friedrich Alexander Universität Erlangen-Nürnberg)*

- **Asynchronous Distributed Key Generation for Computationally-Secure Randomness Consensusand Threshold Signatures.** 1751
  Eleftherios Kokoris Kogias *(Facebook Novi & IST Austria)*,
  Dahlia Malkhi, Alexander Spiegelman *(Facebook Novi)*
- **UC Non-InteractiveProactiveThreshold ECDSA with Identifiable Aborts** 1769
  Ran Canetti *(Boston University)*, Rosario Gennaro *(The City College of New York)*,
  Steven Goldfeder *(Cornell Tech & Offchain Labs)*, Nikolaos Makriyannis, Udi Peled *(Fireblocks)*

Session 6B: Exploitation and Defenses

- **A Generic Technique for Automatically Finding Defense-Aware Code Reuse Attacks** 1789
  Edward J. Schwartz, Cory F. Cohen, Jeffrey S. Gennari *(Carnegie Mellon University)*,
  Stephanie M. Schwartz *(Millersville University)*
- **Methodologies for Quantifying (Re-)randomization Security and Timing under JIT-ROP** .. 1803
  Salman Ahmed, Ya Xiao *(Virginia Tech)*, Kevin Z. Snow *(Zeropoint Dynamics, LLC)*,
  Gang Tan *(Penn State University)*, Fabian Monrose *(University of North Carolina at Chapel Hill)*,
  Danfeng (Daphne) Yao *(Virginia Tech)*
- **Finding Cracks in Shields: On the Security of Control Flow Integrity Mechanisms** 1821
  Yuan Li *(BNRist & INSC, Tsinghua University)*, Mingzhe Wang *(Tsinghua University)*,
  Chao Zhang *(BNRist & INSC, Tsinghua University)*, Xingman Chen, Songtao Yang *(Tsinghua University)*,
  Ying Liu *(BNRist & INSCT, singhua University)*
- **RTFM! Automatic Assumption Discovery and Verification Derivation from Library Document for API Misuse Detection** 1837
  Tao Lv, Ruishi Li, Yi Yang, Kai Chen *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*,
  Xiaojing Lia, XiaoFeng Wang *(Indiana University Bloomington)*,
  Peiwei Hu *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*, Luyi Xing *(Indiana University Bloomington)*

Session 6C: Side Channels

- **InSpectre: Breaking and Fixing Microarchitectural Vulnerabilities by Formal Analysis** 1853
  Roberto Guanciale, Musard Balliu, Mads Dam *(KTH Royal Institute of Technology)*
- **Speculative Probing: Hacking Blind in the Spectre Era** 1871
  Enes Göktas *(Stevens Institute of Technology)*, Kaveh Razavi *(ETH Zurich)*,
  Georgios Portokalidis *(Stevens Institute of Technology)*,
  Herbert Bos, Cristiano Giuffrida *(Vrije Universiteit Amsterdam)*
- **Déjà Vu: Side-Channel Analysis of Mozilla's NSS** 1887
  Sohaib ul Hassan, Iaroslav Gridin, Ignacio M. Delgado-Lozano, Cesar Pereida García,
  Jesús-Javier Chi-Domínguez, Alejandro Cabrera Aldaya, Billy Bob Brumley *(Tampere University)*
- **TRUSTORE: Side-Channel Resistant Storage for SGX using Intel Hybrid CPU-FPGA** 1903
  Hyunyoung Oh *(Seoul National University)*, Adil Ahmad *(Purdue University)*,
  Seonghyun Park, Byoungyoung Lee, Yunheung Paek *(Seoul National University)*

Session 6D: Web Security

- **DECO: Liberating Web Data Using Decentralized Oracles for TLS** 1919
  Fan Zhang, Deepak Maram, Harjasleen Malvai, Steven Goldfeder, Ari Juels
  (Cornell Tech and The Initiative for CryptoCurrencies & Contracts)
- **Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks** 1939
  Mingming Zhang *(Tsinghua University)*, Xiaofeng Zheng *(Tsinghua University & QI-ANXIN Group)*,
  Kaiwen Shen *(Tsinghua University)*, Ziqiao Kong *(QI-ANXIN Group)*,
  Chaoyi Lu, Yu Wang *(Tsinghua University)*, Haixin Duan *(Tsinghua University & QI-ANXIN Group)*,
  Shuang Hao *(University of Texas at Dallas)*, Baojun Liu *(Tsinghua University)*, Min Yang *(Fudan University)*

- **The Cookie Hunter: Automated Black-box Auditing for Web Authentication and Authorization Flaws** 1953
  Kostas Drakonakis *(FORTH ICS)*, Sotiris Ioannidis *(Technical University of Crete)*, Jason Polakis *(University of Illinois at Chicago)*
- **TrafficSliver: Fighting Website Fingerprinting Attacks with Traffic Splitting** 1971
  Wladimir De la Cadena *(University of Luxembourg)*, Asya Mitseva *(Brandenburg Technical University)*,
  Jens Hiller, Jan Pennekamp, Sebastian Reuter, Julian Filter *(RWTH Aachen University)*,
  Thomas Engel *(University of Luxembourg)*, Klaus Wehrle *(RWTH Aachen University)*,
  Andriy Panchenko *(Brandenburg Technical University)*

Session 6E: Zero Knowledge

- **Lift-and-Shift: Obtaining Simulation Extractable Subversion and Updatable SNARKs Generically** 1987
  Behzad Abdolmaleki *(University of Tartu)*,
  Sebastian Ramacher, Daniel Slamanig *(AIT Austrian Institute of Technology)*
- **Pointproofs: Aggregating Proofs for Multiple Vector Commitments** 2007
  Sergey Gorbunov *(University of Waterloo)*, Leonid Reyzin *(Algorand and Boston University)*,
  Hoeteck Wee *(CNRSENSPSL and NTT Research)*, Zhenfei Zhang *(Algorand)*
- **Ligero++: A New Optimized Sublinear IOP** 2025
  Rishabh Bhadauria *(Bar-Ilan University)*, Zhiyong Fang *(Texas A&M University)*,
  Carmit Hazay *(Ligero Inc. & Bar-Ilan University)*,
  Muthuramakrishnan Venkitasubramaniam *(Ligero Inc. & University of Rochester)*,
  Tiancheng Xie *(University of California, Berkeley)*, Yupeng Zhang *(Texas A&M University)*
- **Zero Knowledge Proofs for Decision Tree Predictions and Accuracy** 2039
  Jiaheng Zhang *(University of California, Berkeley)*, Zhiyong Fang, Yupeng Zhang *(Texas A&M University)*,
  Dawn Song *(University of California, Berkeley)*
- **A 2.1 KHz Zero-Knowledge Processor with BubbleRAM** 2055
  David Heath, Vladimir Kolesnikov *(Georgia Institute of Technology)*

Keynote Talk II

- **Realistic Threats and Realistic Users: Lessons from the Election** 2075
  Alex Stamos *(Stanford University)*

Demos

- **Demo: PhishBench 2.0: A Versatile and Extendable Benchmarking Framework for Phishing** 2077
  Victor Zeng, Xin Zhou, Shahryar Baki, Rakesh M. Verma *(University of Houston)*
- **Demo: Benchmarking Label Dynamics of VirusTotal Engines** 2081
  Shuofei Zhu *(Pennsylvania State University)*,
  Ziyi Zhang, Limin Yang *(University of Illinois at Urbana-Champaign)*,
  Linhai Song *(Pennsylvania State University)*, Gang Wang *(University of Illinois at Urbana-Champaign)*
- **Demo: VRLifeTime -- An IDE Tool to Avoid Concurrency and Memory Bugs in Rust** 2085
  Ziyi Zhang *(University of Science and Technology of China & Pennsylvania State University)*,
  Boqin Qin *(Beijing University of Posts and Telecommunications & Pennsylvania State University)*,
  Yilun Chen *(HoneycombData Inc.)*, Linhai Song *(Pennsylvania State University)*,
  Yiying Zhang *(University of CaliforniaSan Diego)*

Posters

- **Poster: LPET -- Mining MS-Windows Software Privilege Escalation Vulnerabilities by Monitoring Interactive Behavior** 2089
  Can Huang, Xinhui Han, Guorui Yu *(Peking University)*

- **Poster: Towards Using Source Code Repositories to Identify Software Supply Chain Attacks** 2093
  Duc Ly Vu, Ivan Pashchenko *(University of Trento),*
  Fabio Massacci *(University of Trento & Vrije Universiteit Amsterdam),*
  Henrik Plate, Antonino Sabetta *(SAP Security Research)*

- **Poster: Cybersecurity Research and Training for Power Distribution Grids -- A Blueprint** .. 2097
  Martin Henze, Lennart Bader *(Fraunhofer FKIE),* Julian Filter *(RWTH Aachen University),*
  Olav Lamberts *(Fraunhofer FKIE & RWTH Aachen University),* Simon Ofner *(Fraunhofer FKIE),*
  Dennis van der Velde *(Fraunhofer FIT)*

- **Poster: Continuous and Multiregional Monitoring of Malicious Hosts** 2101
  Shota Fujii *(HitachiLtd. & Okayama University),* Takayuki Sato, Sho Aoki *(HitachiLtd.),*
  Yu Tsuda *(National Institute of Information and Communications Technology),* Yusuke Okano *(FFRI SecurityInc.),*
  Tomohiro Shigemoto, Nobutaka Kawaguchi, Masato Terada *(HitachiLtd.)*

- **Poster: Facilitating Protocol-independent Industrial Intrusion Detection Systems** 2105
  Konrad Wolsing *(Fraunhofer FKIE & RWTH Aachen University),* Eric Wagner, Martin Henze *(Fraunhofer FKIE)*

- **Poster: Bento: Bringing Network Function Virtualization to Tor** 2109
  Michael Reininger *(University of Maryland),* Arushi Arora *(Purdue University),*
  Stephen Herwig, Nicholas Francino *(University of Maryland),* Christina Garman *(Purdue University),*
  Dave Levin *(University of Maryland)*

- **Poster: RIPT -- An Efficient Multi-Core Record-Replay System** 2113
  Jiashuo Liang, Guancheng Li *(Peking University),*
  Chao Zhang *(Institute for Network Science and Cyberspace of Tsinghua University),*
  Ming Yuan, Xingman Chen *(Tsinghua University),* Xinhui Han *(Peking University)*

- **Poster: Impact of Energy Consumption Attacks on LoRaWAN-Enabled Devices in Industrial Context** 2117
  Muhammad Nouman Nafees, Neetesh Saxena, Pete Burnap *(Cardiff University),*
  Bong Jun Choi *(Soongsil University)*

- **Poster: A Multi-phased Multi-faceted IoT Honeypot Ecosystem** 2121
  Armin Ziaie Tabari, Xinming Ou *(University of South Florida)*

- **Poster: Voice-Indistinguishability -- Protecting Voiceprint with Differential Privacy under an Untrusted Server** 2125
  Yaowei Han, Yang Cao *(Kyoto University),*
  Sheng Li *(National Institute of Information and Communications Technology),*
  Qiang Ma, Masatoshi Yoshikawa *(Kyoto University)*

- **Poster: rProfiler — Assessing Insider Influence on Enterprise Assets** 2129
  Manish Shukla, Sachin Lodha *(TCS Research Lab)*

Workshops

- **CCSW'20: 2020 Cloud Computing Security Workshop** 2133
  Radu Sion *(Stony Brook University),* Yinqian Zhang *(The Ohio State University)*

- **CPSIOTSEC'20: 2020 Joint Workshop on CPS&IoT Security and Privacy** 2135
  Michail Maniatakos *(New York University Abu Dhabi),*
  Yuqing Zhang *(University of Chinese Academy of Sciences)*

- **MTD'20: 7th ACM Workshop on Moving Target Defense** 2137
  Hamed Okhravi *(MIT Lincoln Laboratory),* Cliff Wang *(Army Research Office)*

- **PPMLP 2020: Workshop on Privacy-Preserving Machine Learning In Practice** 2139
  Benyu Zhang *(Ant Group),* Matei Zaharia *(Stanford University),* Shouling Ji *(Zhejiang University),*
  Raluca Ada Popa *(University of California, Berkeley),* Guofei Gu *(Texas A&M University)*

- **19th Workshop on Privacy in the Electronic Society (WPES 2020)** 2141
  Wouter Lueks *(École Polytechnique Fédérale de Lausanne),* Paul Syverson *(U.S. Naval Research Laboratory)*

- **AISec'20: 13th Workshop on Artificial Intelligence and Security** 2143
  Sadia Afroz *(University of California, Berkeley & Avast),* Nicholas Carlini *(Google Brain),*
  Ambra Demontis *(University of Cagliari)*

- **ASHES 2020: 4th Workshop on Attacks and Solutions in Hardware Security** 2145
  Chip Hong Chang *(NTU)*, Stefan Katzenbeisser *(University of Passau)*,
  Ulrich Rührmair *(LMU Munich and University of Connecticut)*,
  Patrick Schaumont *(Worcester Polytechnic Institute)*
- **2nd Workshop on Cyber-Security Arms Race (CYSARM 2020)** 2147
  Thanassis Giannetsos *(Technical University of Denmark)*,
  Daniele Sgandurra *(Royal HollowayUniversity of London)*
- **FEAST'20: Fifth Workshop on Forming an Ecosystem Around Software Transformation** 2149
  Kevin W. Hamlen *(The University of Texas at Dallas)*, Long Lu *(Northeastern University)*
- **PLAS'20: 15th Workshop on Programming Languages and Analysis for Security** 2151
  Alley Stoughton *(Boston University)*, Marco Vassena *(CISPA Helmholtz Center for Information Security)*
- **TPDP'20: 6th Workshop on Theory and Practice of Differential Privacy** 2153
  Rachel Cummings *(Georgia Institute of Technology)*, Michael Hay *(Colgate University)*

Author Index 2155

CCS 2020 Conference Organization

General Chairs:	Jay Ligatti (University of South Florida, USA)
	Xinming Ou (University of South Florida, USA)
Program Chairs:	Jonathan Katz (University of Maryland, USA)
	Giovanni Vigna (University of California-Santa Barbara, USA)
Web Chair:	Armin Ziaie Tabari (University of South Florida, USA)
Treasurer:	Alexandru Bardas (University of Kansas, USA)
Publication Chairs:	Mehran Mozaffari Kermani (University of South Florida, USA)
	Ryan Gerdes (Virginia Tech, USA)
Sponsorship Chairs:	Weidong Cui (Microsoft)
	Amir Rahmati (Stony Brook University, USA)
	Raj Rajagopalan (Resideo)
Registration Chairs:	Amro Awad (North Carolina State University, USA)
	Cliff Zou (University of Central Florida, USA)
Workshop Chair:	Gang Tan (Pennsylvania State University, USA)
Publicity Chairs:	Bo Luo (University of Kansas, USA)
	Xiaoyan Sun (California State University, USA)
Student Conference Grant Chairs:	Fengjun Li (University of Kansas, USA)
	Wenjing Lou (Virginia Tech, USA)
	Daniel Takabi (Georgia State University, USA)
Poster/Demo Chair:	Anna Cinzia Squicciarini (Pennsylvania State University, USA)
Virtual Conference Task Force:	Paul Gazzillo (Chair) (University of Central Florida, USA)
	Alexandru Bardas (University of Kansas, USA)
	Armin Ziaie Tabari (University of South Florida, USA)
	Shiyi Wei (University of Texas at Dallas, USA)
	Mohammed Abuhamad (Loyola University Chicago, USA)
	Afsah Anwar (University of Central Florida, USA)
	JinChun Choi (Texas A&M University-Kingsville, USA)
Steering Committee:	Somesh Jha (Chair) (University of Wisconsin-Madison)
	Rebecca Wright (Barnard College)
	Carl Landwehr (George Washington University)
	Trent Jaeger (Pennsylvania State University)
	Stefan Savage (University of California-San Diego)
	David Basin (ETH Zurich)

Program Committee Area Chairs:

Applied Cryptography
Benny Pinkas (Bar Ilan University)
Blockchain and Distributed Systems
Vassilis Zikas (University of Edinburgh)
Formal Methods and Programming-Language Security
Deepak Garg (Max Planck Institute for Software Systems)
Hardware Security and Side Channels
Herbert Bos (Vrije Universiteit Amsterdam)
Machine Learning and Security
Prateek Saxena (National University of Singapore)
Network Security
Cristina Nita-Rotaru (Northeastern University)
Privacy and Censorship
Ashwin Machanavajjhala (Duke University)
Software and Web Security
Engin Kirda (Northeastern University)
Usability and Measurement
Serge Egelman (University of California-Berkeley)

Program Committee Members:

AbdelRahman Abdou (Carleton University)
Manos Antonakakis (Georgia Institute of Technology)
Aslan Askarov (Aarhus University)
Michael Backes (CISPA Helmholtz Center for Information Security)
Foteini Baldimtsi (George Mason University)
Davide Balzarotti (Eurecom)
Tiffany Bao (Arizona State University)
Gilles Barthe (MPI-SP and IMDEA)
Adam Bates (University of Illinois at Urbana-Champaign)
Iddo Bentov (Cornell Tech)
Karthikeyan Bhargavan (INRIA)
Antonio Bianchi (Purdue University)
Leyla Bilge (NortonLifeLock Research Group)
Bruno Blanchet (Inria)
Jonathan Bootle (IBM Research – Zurich)
Kevin Borgolte (Princeton University)
Kevin Butler (University of Florida)
Juan Caballero (IMDEA Software Institute)
Matthew Caesar (University of Illinois at Urbana-Champaign)
Yinzhi Cao (Johns Hopkins University)
Lorenzo Cavallaro (King's College London)
Hao Chen (Microsoft Research)
Yaohui Chen (Facebook)
Nicolas Christin (Carnegie Mellon University)

Program Committee Members (continued):

Mihai Christodorescu (Visa Research)
Gabriela Ciocarlie (SRI International)
Andrea Continella (UC Santa Barbara/University of Twente)
Véronique Cortier (CNRS, Loria, France)
Cas Cremers (CISPA Helmholtz Center for Information Security)
Weidong Cui (Microsoft Research)
Rachel Cummings (Georgia Institute of Technology)
George Danezis (UCL / Facebook Calibra)
Lucas Davi (University of Duisburg-Essen)
Srini Devadas (MIT)
Adam Doupé (Arizona State University)
Tudor Dumitras (University of Maryland, College Park)
François Dupressoir (University of Bristol)
Manuel Egele (Boston University)
Karim Eldefrawy (SRI Internationa)
Nick Feamster (University of Chicago)
Earlence Fernandes (University of Wisconsin-Madison)
Tobias Fiebig (TU Delft)
Aurélien Francillon (Eurecom)
Michael Franz (University of California, Irvine)
Yanick Fratantonio (EURECOM)
Matt Fredrikson (CMU)
Alisa Frik (ICSI / UC Berkeley)
Marco Gaboardi (Boston University)
Daniel Genkin (University of Michigan)
Esha Ghosh (Microsoft Research, Redmond, USA)
Cristiano Giuffrida (VU Amsterdam)
Neil Gong (Duke University)
Dov Gordon (George Mason University)
Guofei Gu (Texas A&M University)
Trinabh Gupta (UC Santa Barbara)
Xi He (University of Waterloo)
Amir Herzberg (University of Connecticut)
Amir Houmansadr (UMass Amherst)
Suman Jana (Columbia University)
L Jean Camp (Indiana University)
Somesh Jha (University of Wisconsin, Madison)
Sanjay Jha (UNSW Sydney)
Aaron Johnson (U.S. Naval Research Laboratory)
Murat Kantarcioglu (University of Texas at Dallas)
Alexandros Kapravelos (North Carolina State University)
Aggelos Kiayias (University of Edinburgh and IOHK)
Daniel Kifer (Penn State University)

Program Committee Members (continued):

Yongdae Kim (KAIST)
Katharina Krombholz (CISPA Helmholtz Center for Info. Security)
Wenke Lee (Georgia Institute of Technology)
Dave Levin (University of Maryland)
Ninghui Li (Purdue University)
Zhou Li (UC Irvine)
David Lie (University of Toronto)
Zhiqiang Lin (Ohio State University)
Martina Lindorfer (TU Wien)
Peng Liu (Penn State University)
Kangjie Lu (University of Minnesota)
Loi Luu (Kyber Network)
Shiqing Ma (Rutgers University)
Matteo Maffei (TU Wien)
Piotr Mardziel (Carnegie Mellon University)
Stephen McCamant (University of Minnesota)
Patrick McDaniel (Penn State University)
Jiang Ming (University of Texas at Arlington)
Jelena Mirkovic (USC Information Sciences Institute)
Z. Morley Mao (University of Michigan)
Andrew Myers (Cornell University)
Kartik Nayak (Duke University)
Nick Nikiforakis (Stony Brook University)
Peng Ning (Google)
Ariel Nof (Technion)
Catuscia Palamidessi (INRIA)
Nicolas Papernot (University of Toronto and Vector Institute)
Paul Pearce (Georgia Tech)
Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security)
Roberto Perdisci (University of GA and Georgia Institute of Technology)
Frank Piessens (KU Leuven)
Jason Polakis (University of Illinois at Chicago)
Michalis Polychronakis (Stony Brook University)
Georgios Portokalidis (Stevens Institute of Technology)
Sara Rampazzi (University of Michigan)
Aanjhan Ranganathan (Northeastern University)
Aseem Rastogi (Microsoft Research)
Mariana Raykova (Google)
Kaveh Razavi (Vrije Universiteit Amsterdam)
Michael Reiter (UNC-Chapel Hill)
Ling Ren (University of Illinois Urbana Champaign)
Konrad Rieck (TU Braunschweig)
Peter Rindal (Visa Research)

Program Committee Members (continued):

William Robertson (Northeastern University)
Andrei Sabelfeld (Chalmers)
Brendan Saltaformaggio (Georgia Institute of Technology)
David Sands (Chalmers)
Nolen Scaife (University of Colorado Boulder)
Jörg Schwenk (Ruhr University Bochum)
Reza Shokri (National University of Singapore)
Yan Shoshitaishvili (Arizona State University)
Radu Sion (Private Machines Inc and Stony Brook University)
Alex C. Snoeren (UC San Diego)
Ben Stock (CISPA Helmholtz Center for Information Security)
Alley Stoughton (Boston University)
Gianluca Stringhini (Boston University)
Min Suk Kang (National University of Singapore)
Yixin Sun (University of Virginia)
Mohit Tiwari (UT Austin and Symmetry Systems)
Jonathan Ullman (Northeastern University)
Blase Ur (University of Chicago)
Narseo Vallina-Rodriguez (IMDEA Networks/ICSI)
Erik van der Kouwe (Vrije Universiteit Amsterdam)
Venkat Venkatakrishnan (UIC)
Muthuramakrishnan Venkitasubramaniam (University of Rochester)
Ruoyu “Fish” Wang (Arizona State University)
Xiao Wang (Northwestern University)
XiaoFeng Wang (Indiana University)
Ting Wang (Pennsylvania State University)
Xusheng Xiao (Case Western Reserve University)
Xiaokui Xiao (National University of Singapore)
Xinyu Xing (Penn State University)
Luyi Xing (Indiana University Bloomington)
Daniel Zappala (Brigham Young University)
Fengwei Zhang (SUSTech)
Yinqian Zhang (Ohio State University)
Xiangyu Zhang (Purdue University)
Danfeng Zhang (Penn State University)
Yang Zhang (CISPA Helmholtz Center for Information Security)

ACM CCS 2020 Sponsor & Supporters

Sponsor: acm SIGSAC

Platinum Supporters: NSF vmware®

Gold Supporters: ANT GROUP Google IBM. intel® Microsoft

Silver Supporters: FACEBOOK paloalto® NETWORKS

Bronze Supporters: Baidu USA PlatON