**Accepted Papers**

You can find the proceedings [here](https://www.computer.org/csdl/proceedings/sp/2022/1wKCdeg89vq).

**"Adversarial Examples for Proof-of-Learning"**   
Rui Zhang (Zhejiang University), Jian Liu (Zhejiang University), Yuan Ding (Zhejiang University), Zhibo Wang (Zhejiang University), Qingbiao Wu (Zhejiang University), Kui Ren (Zhejiang University), Jian Liu (Zhejiang University)

**"Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya**   
Collins W. Munyendo (The George Washington University), Yasemin Acar (The George Washington University), Adam J. Aviv (The George Washington University), Yasemin Acar (George Washington University)

**"Flawed, but like democracy we don't have a better system": The Experts' Insights on the Peer Review Process of Evaluating Security Papers**   
Ananta Soneji (Arizona State University), Faris Bugra Kokulu (Arizona State University), Carlos Rubio-Medrano (Texas A&M University - Corpus Christi), Tiffany Bao (Arizona State University), Ruoyu Wang (Arizona State University), Yan Shoshitaishvili (Arizona State University), Adam Doupe (Arizona State University)

**"They're not that hard to mitigate": What Cryptographic Library Developers Think About Timing Attacks**   
Jan Jancar (Masaryk University), Marcel Fourné (Max Planck Institute for Security and Privacy), Daniel De Almeida Braga (Univ Rennes, CNRS, IRISA), Mohamed Sabt (Univ Rennes, CNRS, IRISA), Peter Schwabe (Max Planck Institute for Security and Privacy & Radboud University), Gilles Barthe (Max Planck Institute for Security and Privacy & IMDEA Software Institute), Pierre-Alain Fouque (Univ Rennes, CNRS, IRISA), Yasemin Acar (Max Planck Institute for Security and Privacy & George Washington University)

**27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University**   
Christian Stransky (Leibniz University Hannover, Germany), Oliver Wiese (Freie Universität Berlin, Germany), Volker Roth (Freie Universität Berlin, Germany), Yasemin Acar (Max Planck Institute for Security and Privacy, Germany), Sascha Fahl (CISPA / Leibniz University Hannover, Germany)

**A Formal Security Analysis of the W3C Web Payment APIs: Attacks and Verification**   
Quoc Huy Do (University of Stuttgart, Germany), Pedram Hosseyni (University of Stuttgart, Germany), Ralf Küsters (University of Stuttgart, Germany), Guido Schmitz (University of Stuttgart, Germany and Royal Holloway, University of London, UK), Nils Wenzler (University of Stuttgart, Germany), Tim Würtele (University of Stuttgart, Germany)

**A Logic and an Interactive Prover for the Computational Post-Quantum Security of Protocols**   
Cas Cremers (CISPA Helmholtz Center for Information Security), Charlie Jacomme (CISPA - Helmholtz Center for Information Security), Caroline Fontaine (Université Paris-Saclay, CNRS, ENS Paris-Saclay, Laboratoire Méthodes Formelles), Cas Cremers (CISPA Helmholtz Center for Information Security)

**A Secret-Free Hypervisor: Rethinking Isolation in the Age of Speculative Vulnerabilities**   
Hongyan Xia (Microsoft Research), David Zhang (Microsoft), Wei Liu (Microsoft), Istvan Haller (Microsoft Research), Bruce Sherwin (Microsoft), David Chisnall (Microsoft Research)

**A Systematic Look at Ciphertext Side Channels on AMD SEV-SNP**   
Mengyuan Li (The Ohio State University), Luca Wilke (University of Lübeck), Jan Wichelmann (University of Lübeck), Thomas Eisenbarth (University of Lübeck), Radu Teodorescu (The Ohio State University), Yinqian Zhang (Southern University of Science and Technology)

**AccEar: Accelerometer Acoustic Eavesdropping with Unconstrained Vocabulary**   
Pengfei Hu (Shandong University), Hui Zhuang (Shandong University), Panneer Selvam Santhalingam (George Mason University), Riccardo Spolaor (Shandong University), Parth Pathak (George Mason University), Guoming Zhang (Shandong University), Xiuzhen Cheng (Shandong University)

**Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks**   
Yanan Guo (University of Pittsburgh), Andrew Zigerelli (Independent), Youtao Zhang (Computer Science Department, University of Pittsburgh), Jun Yang (University of Pittsburgh)

**Analyzing Ground-Truth Data of Mobile Gambling Scam**   
Geng Hong (Fudan University), Zhemin Yang (Fudan University), Sen Yang (Fudan University), Xiaojing Liao (Indiana University Bloomington), Xiaolin Du (Fudan University), Min Yang (Fudan University), Haixin Duan (Institute for Network Science and Cyberspace, Tsinghua University; Qi An Xin Group Corp.)

**Annotating, Tracking, and Protecting Cryptographic Secrets with CryptoMPK**   
Xuancheng Jin (Shanghai Jiao Tong University), Xuangan Xiao (Shanghai Jiao Tong University), Songlin Jia (Shanghai Jiao Tong University), Wang Gao (Shanghai Jiao Tong University), Hang Zhang (UC Riverside), Dawu Gu (Shanghai Jiao Tong University), Siqi Ma (The University of Queensland), Zhiyun Qian (UC Riverside), Juanru Li (Shanghai Jiao Tong University)

**Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems**   
Paul Staat (Max Planck Institute for Security and Privacy), Johannes Tobisch (Max Planck Institute for Security and Privacy), Christian Zenger (PHYSEC GmbH), Christof Paar (Max Planck Institute for Security and Privacy)

**Are We There Yet? Timing and Floating-Point Attacks on Differential Privacy Systems**   
Jiankai Jin (The University of Melbourne, Australia), Eleanor McMurtry (ETH Zurich), Benjamin Rubinstein (University of Melbourne, Australia), Olga Ohrimenko (The University of Melbourne)

**Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions**   
Hammond Pearce (NYU Tandon School of Engineering), Baleegh Ahmad (NYU Tandon School of Engineering), Benjamin Tan (NYU Tandon School of Engineering), Brendan Dolan-Gavitt (NYU Tandon School of Engineering), Ramesh Karri (NYU Tandon School of Engineering)

**Attacks on Wireless Coexistence**   
Jiska Classen (TU Darmstadt, SEEMOO), Michael Hermann (TU Darmstadt, SEEMOO), Francesco Gringoli (University of Brescia), Matthias Hollick (TU Darmstadt, SEEMOO)

**Augury: Using Data Memory-Dependent Prefetchers to Leak Data at Rest**   
Jose Rodrigo Sanchez Vicarte (University of Illinois at Urbana-Champaign), Michael Flanders (University of Washington), Riccardo Paccagnella (University of Illinois at Urbana-Champaign), Grant Garrett-Grossman (University of Illinois at Urbana-Champaign), Adam Morrison (Tel Aviv University), Chris Fletcher (University of Illinois at Urbana-Champaign), David Kohlbrenner (University of Washington)

**Automated Attack Synthesis by Extracting Finite State Machines from Protocol Specification Documents**   
Maria Pacheco Gonzales (Purdue University), Max von Hippel (Northeastern University), Ben Weintraub (Northeastern University), Dan Goldwasser (Purdue University), Cristina Nita-Rotaru (Northeastern University)

**BEACON : Directed Grey-Box Fuzzing with Provable Path Pruning**   
Heqing Huang (The Hong Kong University of Science and Technology), Yiyuan Guo (The Hong Kong University of Science and Technology), Qingkai Shi (The Hong Kong University of Science and Technology), Peisen Yao (The Hong Kong University of Science and Technology), Rongxin Wu (Xiamen University), Charles Zhang (The Hong Kong University of Science and Technology)

**Back to the Drawing Board: A Critical Evaluation of Poisoning Attacks on Federated Learning**   
Virat Shejwalkar (UMass Amherst), Amir Houmansadr (UMass Amherst), Peter Kairouz (Google), Daniel Ramage (Google)

**Bad Characters: Imperceptible NLP Attacks**   
Nicholas Boucher (University of Cambridge), Ilia Shumailov (University of Cambridge, Vector Institute), Ross Anderson (University of Cambridge, University of Edinburgh), Nicolas Papernot (University of Toronto, Vector Institute)

**BadEncoder: Backdoor Attacks to Pre-trained Encoders in Self-Supervised Learning**   
Jinyuan Jia (Duke University, USA), Yupei Liu (Duke University, USA), Neil Zhenqiang Gong (Duke University, USA)

**Blacksmith: Compromising Target Row Refresh by Rowhammering in the Frequency Domain**   
Patrick Jattke (ETH Zurich), Victor van der Veen (Qualcomm Technologies Inc.), Pietro Frigo (Vrije Universiteit Amsterdam), Stijn Gunter (ETH Zurich), Kaveh Razavi (ETH Zurich)

**COBRA: Dynamic Proactive Secret Sharing for Confidential BFT Services**   
Robin Vassantlal (LASIGE, Faculdade de Ciencias, Universidade de Lisboa), Eduardo Alchieri (Universidade de Brasilia), Bernardo Ferreira (LASIGE, Faculdade de Ciencias, Universidade de Lisboa), Alysson Bessani (LASIGE, Faculdade de Ciencias, Universidade de Lisboa)

**Cats vs. Spectre: An Axiomatic Approach to Modeling Speculative Execution Attacks**   
Hernán Ponce de León (Bundeswehr University Munich), Johannes Kinder (Bundeswehr University Munich)

**CirC: Compiler infrastructure for proof systems, software verification, and more**   
Alex Ozdemir (Stanford University), Fraser Brown (Stanford University, Carnegie Mellon University), Riad Wahby (Stanford University, Carnegie Mellon University, and Algorand), Alex Ozdemir (Stanford University)

**Committed to Trust: A Qualitative Study on Security & Trust in Open Source Software Projects**   
Dominik Wermke (CISPA Helmholtz Center for Information Security), Noah Woehler (CISPA Helmholtz Center for Information Security), Jan H. Klemmer (Leibniz University Hannover), Marcel Fourné (Max Planck Institute for Security and Privacy), Yasemin Acar (George Washington University), Sascha Fahl (CISPA Helmholtz Center for Information Security, Leibniz University Hannover)

**Copy, Right? A Testing Framework for Copyright Protection of Deep Learning Models**   
Jialuo Chen (Zhejiang University), Jingyi Wang (Zhejiang University), Tinglan Peng (Zhejiang University), Youcheng Sun (Queen's University Belfast, UK), Peng Cheng (Zhejiang University), Shouling Ji (Zhejiang University), Xingjun Ma (Deakin University), Bo Li (University of Illinois Urbana-Champaign), Dawn Song (University of California, Berkeley)

**DEPCOMM: Graph Summarization on System Audit Logs for Attack Investigation**   
Zhiqiang Xu (Chinese Academy of Sciences, China), Pengcheng Fang (Case Western Reserve University, USA), Changlin Liu (Case Western Reserve University, USA), Xusheng Xiao (Case Western Reserve University, USA), Yu Wen (Chinese Academy of Sciences, China), Dan Meng (Chinese Academy of Sciences, China)

**DeepCASE: Semi-Supervised Contextual Analysis of Security Events**   
Thijs van Ede (University of Twente), Hojjat Aghakhani (University of California, Santa Barbara), Noah Spahn (University of California, Santa Barbara), Riccardo Bortolameotti (ReaQta), Marco Cova (VMware, Inc.), Andrea Continella (University of Twente), Maarten van Steen (University of Twente), Andreas Peter (University of Twente), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California)

**DeepCoFFEA: Improved Flow Correlation Attacks on Tor via Metric Learning and Amplification**   
Se Eun Oh (Ewha Womans University), Taiji Yang (University of Minnesota), Nate Mathews (Rochester Institute of Technology), James K Holland (University of Minnesota), Mohammad Saidur Rahman (Rochester Institute of Technology), Nicholas Hopper (University of Minnesota), Matthew Wright (Rochester Institute of Technology)

**DeepSteal: Advanced Model Extractions Leveraging Efficient Weight Stealing in Memories**   
Adnan Siraj Rakin (Arizona State University), Md Hafizul Islam Chowdhuryy (University of Central Florida), Fan Yao (University of Central Florida), Deliang Fan (Arizona State University)

**Delay Wreaks Havoc on Your Smart Home: Delay-based Automation Interference Attacks**   
Haotian Chi (Temple University), Chenglong Fu (Temple University), Qiang Zeng (University of South Carolina, United States of America), Xiaojiang Du (Stevens Institute of Technology)

**Deployment of Source Address Validation by Network Operators: A Randomized Control Trial**   
Qasim Lone (Delft University of Technology), Alisa Frik (International Computer Science Institute / UC Berkeley), Matthew Luckie (University of Waikato), Maciej Korczynski (Grenoble INP), Michel van Eeten (Delft University of Technology), Carlos Ganan (Delft University of Technology)

**Device Fingerprinting with Peripheral Timestamps**   
John Monaco (Naval Postgraduate School, USA)

**Differential Privacy and Swapping: Examining De-Identification's Impact on Minority Representation and Privacy Preservation in the U.S. Census**   
Sarah Radway (Tufts University), Miranda Christ (Columbia University), Steven Bellovin (Columbia University)

**Differentially Private Histograms in the Shuffle Model from Fake Users**   
Albert Cheu (Georgetown University), Maxim Zhilyaev (MindStrong Inc.)

**Domains Do Change Their Spots: Quantifying Potential Abuse of Residual Trust**   
Johnny So (Stony Brook University, USA), Najmeh Miramirkhani (Stony Brook University, USA), Michael Ferdman (Stony Brook University, USA), Nick Nikiforakis (Stony Brook University, USA)

**Effective Seed Scheduling for Fuzzing with Graph Centrality Analysis**   
Dongdong She (Columbia University), Abhishek Shah (Columbia University), Suman Jana (Columbia University)

**Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices**   
Hadi Givehchian (UC San Diego), Nishant Bhaskar (UC San Diego), Eliana Rodriguez Herrera (UC San Diego), Hector Lopez Soto (UC San Diego), Christian Dameff (UC San Diego), Dinesh Bharadia (UC San Diego), Aaron Schulman (UC San Diego)

**Exploit the Last Straw That Breaks Android Systems**   
Lei Zhang (Fudan University, China), Keke Lian (Fudan University, China), Haoyu Xiao (Fudan University, China), Zhibo Zhang (Fudan University, China), Peng Liu (The Pennsylvania State University, United States of America), Yuan Zhang (Fudan University, China), Min Yang (Fudan University, China), Haixin Duan (Tsinghua University, China)

**Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices**   
Takayuki Sasaki (Yokohama National University), Akira Fujita (Yokohama National University/National Institute of Information and Communications Technology), Carlos Hernandez Ganan (TU Delft/Yokohama National University), Michel van Eeten (TU Delft/Yokohama National University), Katsunari Yoshioka (Yokohama National University), Tsutomu Matsumoto (Yokohama National University)

**FSAFlow: Lightweight and Fast Dynamic Path Tracking and Control for Privacy Protection on Android Using Hybrid Analysis with State-Reduction Strategy**   
Zhi Yang (PLA Information Engineering University, Zhengzhou, China), Zhanhui Yuan (PLA Information Engineering University, Zhengzhou, China), Xingyuan Chen (PLA Information Engineering University, Zhengzhou, China), Shuyuan Jin (SUN YAT-SEN University, Guangzhou, China.), Lei Sun (PLA Information Engineering University, Zhengzhou, China), Xuehui Du (PLA Information Engineering University, Zhengzhou, China), Wenfa Li (Beijing Union University, Beijing, Chian)

**Finding SMM Privilege-Escalation Vulnerabilities in UEFI Firmware with Protocol-Centric Static Analysis**   
Jiawei Yin (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China), Wei Huo (Key Laboratory of Network Assessment Technology, Institute of Information Engineering, Chinese Academy of Sciences, China; School of CyberSpace Security at University of Chinese Academy of Sciences, China), Menghao Li (Institute of Information Engineering, Chinese Academy of Sciences), Wei Wu (Huawei Technologies), Dandan Sun (Key Laboratory of Network Assessment Technology, Institute of Information Engineering, Chinese Academy of Sciences, China), Jianhua Zhou (Key Laboratory of Network Assessment Technology, Institute of Information Engineering, Chinese Academy of Sciences, China), Jingling Xue (University of New South Wales)

**Finding and Exploiting CPU Features using MSR Templating**   
Andreas Kogler (Graz University of Technology), Daniel Weber (CISPA Helmholtz Center for Information Security), Martin Haubenwallner (Graz University of Technology), Moritz Lipp (Graz University of Technology), Daniel Gruss (Graz University of Technology), Michael Schwarz (CISPA Helmholtz Center for Information Security), Moritz Lipp (Amazon Web Services)

**Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities**   
Jianliang Wu (Purdue University), Ruoyu Wu (Purdue University), Dongyan Xu (Purdue University), Dave (Jing) Tian (Purdue University), Antonio Bianchi (Purdue University)

**Foundations of Dynamic BFT**   
Sisi Duan (Tsinghua University), Haibin Zhang (independent)

**Four Attacks and a Proof for Telegram**   
Martin R. Albrecht (Royal Holloway, University of London, United Kingdom), Lenka Mareková (Royal Holloway, University of London, United Kingdom), Kenneth G. Paterson (ETH Zurich, Switzerland), Igors Stepanovs (ETH Zurich, Switzerland)

**FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks**   
Kyungtae Kim (Purdue University), Taegyu Kim (Purdue University), Ertza Warraich (Purdue University), Byoungyoung Lee (Seoul National University), Kevin Butler (University of Florida), Antonio Bianchi (Purdue University), Dave (Jing) Tian (Purdue University)

**GREBE: Unveiling Exploitation Potential for Linux Kernel Bugs**   
Zhenpeng Lin (Pennsylvania State University), Yueqi Chen (Pennsylvania State University), Dongliang Mu (Huazhong University of Science and Technology), Chensheng Yu (George Washington University), Yuhang Wu (Pennsylvania State University), Xinyu Xing (Pennsylvania State University), Kang Li (Baidu Security)

**Goshawk: Hunting Memory Corruptions via Structure-Aware and Object-Centric Memory Operation Synopsis**   
Yunlong Lyu (University of Science and Technology of China), Yi Fang (Feiyu Security), Yiwei Zhang (Shanghai Jiao Tong University), Qibin Sun (University of Science and Technology of China), Siqi Ma (The University of New South Wales Canberra), Elisa Bertino (Purdue University), Kangjie Lu (University of Minnesota), Juanru Li (Shanghai Jiao Tong University)

**Graphics Peeping Unit: Exploiting EM Side-Channel Information of GPUs to Eavesdrop on Your Neighbors**   
Zihao Zhan (Vanderbilt University), Zhengkai Zhang (Clemson University), Sisheng Liang (Clemson University), Fan Yao (University of Central Florida), Xenofon Koutsoukos (Vanderbilt University)

**HAMRAZ: Resilient Partitioning and Replication**   
Xiao Li (University of California, Riverside, USA), Farzin Houshmand (University of California, Riverside, USA), Mohsen Lesani (University of California, Riverside, USA)

**HardLog: Practical Tamper-Proof System Auditing Using a Novel Audit Device**   
Adil Ahmad (Purdue), Sangho Lee (Microsoft Research), Marcus Peinado (Microsoft Research)

**Hardening Circuit-Design IP Against Reverse-Engineering Attacks**   
Animesh Chhotaray (University of Florida, USA), Thomas Shrimpton (University of Florida, USA)

**Hark: A Deep Learning System for Navigating Privacy Feedback at Scale**   
Hamza Harkous (Google Inc.), Sai Teja Peddinti (Google Inc.), Rishabh Khandelwal (University of Wisconsin - Madison), Animesh Srivastava‚Äé (Google Inc.), Nina Taft (Google Inc.)

**Heapster: Analyzing the Security of Dynamic Allocators for Monolithic Firmware Images**   
Fabio Gritti (University of California, Santa Barbara), Fabio Pagani (University of California, Santa Barbara), Ilya Grishchenko (University of California, Santa Barbara), Lukas Dresel (University of California, Santa Barbara), Nilo Redini (Qualcomm Inc.), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara)

**How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study**   
Marco Gutfleisch (Ruhr University Bochum, Germany), Jan H. Klemmer (Leibniz University Hannover, Germany), Niklas Busch (Leibniz University Hannover, Germany), Yasemin Acar (Max Planck Institute for Security and Privacy, Germany), M. Angela Sasse (Ruhr University Bochum, Germany), Sascha Fahl (CISPA / Leibniz University Hannover, Germany)

**How Not to Protect Your IP - An Industry-Wide Break of IEEE 1735 Implementations**   
Julian Speith (Max Planck Institute for Security and Privacy), Florian Schweins (Ruhr-University Bochum), Maik Ender (Max Planck Institute for Security and Privacy), Marc Fyrbiak (Max Planck Institute for Security and Privacy), Alexander May (Ruhr-University Bochum), Christof Paar (Max Planck Institute for Security and Privacy)

**How to Attack and Generate Honeywords**   
Ding Wang (Nankai University), Yunkai Zou (Nankai University), Qiying Dong (Nankai University), Yuanming Song (Peking University), Xinyi Huang (Fujian Normal University)

**IRQDebloat: Reducing Driver Attack Surface in Embedded Devices**   
Zhenghao Hu (New York University), Brendan Dolan-Gavitt (NYU)

**IRShield: A Countermeasure Against Adversarial Physical-Layer Wireless Sensing**   
Paul Staat (Max Planck Institute for Security and Privacy), Simon Mulzer (Ruhr University Bochum), Stefan Roth (Ruhr University Bochum), Veelasha Moonsamy (Ruhr University Bochum), Markus Heinrichs (TH Köln – University of Applied Sciences, Cologne, Germany), Rainer Kronberger (TH Köln – University of Applied Sciences, Cologne, Germany), Aydin Sezgin (Ruhr University Bochum), Christof Paar (Max Planck Institute for Security and Privacy)

**Investigating Influencer VPN Ads on YouTube**   
Omer Akgul (University of Maryland), Richard Roberts (University of Maryland), Moses Namara (Clemson University), Dave Levin (University of Maryland), Michelle L. Mazurek (University of Maryland)

**Invisible Finger: Practical Electromagnetic Interference Attack on Touchscreen-based Electronic Devices**   
Haoqi Shan (University of Florida), Boyi Zhang (University of Florida), Zihao Zhan (University of Florida), Dean Sullivan (University of New Hampshire), Shuo Wang (University of Florida), Yier Jin (University of Florida)

**IronMask: Versatile Verification of Masking Security**   
Sonia Belaid (CryptoExperts), Darius Mercadier (CryptoExperts), Matthieu Rivain (CryptoExperts), Abdul Rahman Taleb (CryptoExperts)

**Jigsaw: Efficient and Scalable Path Constraints Fuzzing**   
Ju Chen (UC, Riverside), Jinghan Wang (UC, Riverside), Chengyu Song (UC, Riverside), Heng Yin (UC, Riverside)

**LinkTeller: Recovering Private Edges from Graph Neural Networks via Influence Analysis**   
Fan Wu (University of Illinois at Urbana-Champaign, USA), Yunhui Long (University of Illinois at Urbana-Champaign, USA), Ce Zhang (ETH Zurich, Switzerland), Bo Li (University of Illinois at Urbana-Champaign, USA)

**Locally Differentially Private Sparse Vector Aggregation**   
Mingxun Zhou (Carnegie Mellon University), Tianhao Wang (Carnegie Mellon University and University of Virginia), T-H. Hubert Chan (The University of Hong Kong), Giulia Fanti (Carnegie Mellon University), Elaine Shi (Carnegie Mellon University)

**Low-Bandwidth Threshold ECDSA via Pseudorandom Correlation Generators**   
Damiano Abram (Aarhus University), Ariel Nof (Technion), Claudio Orlandi (Aarhus University), Peter Scholl (Aarhus University), Omer Shlomovits (ZenGo X)

**MatRiCT+: More Efficient Post-Quantum Private Blockchain Payments**   
Muhammed F. Esgin (Monash University and CSIRO's Data61, Australia), Ron Steinfeld (Monash University, Australia), Raymond K. Zhao (Monash University, Australia)

**Measuring and Mitigating the Risk of IP Reuse on Public Clouds**   
Eric Pauley (Pennsylvania State University), Ryan Sheatsley (Pennsylvania State University), Blaine Hoak (Pennsylvania State University), Quinn Burke (Pennsylvania State University), Yohan Beugin (Pennsylvania State University), Patrick McDaniel (Pennsylvania State University)

**Membership inference attacks from first principles**   
Nicholas Carlini (Google Brain), Steve Chien (Google Brain), Milad Nasr (UMASS), Shuang Song (Google Research, Brain), Andreas Terzis (Google, Inc.), Florian Tramer (Google Brain)

**MeshUp: Stateless Cache Side-channel Attack on CPU Mesh**   
Junpeng Wan (Fudan University), Yanxiang Bi (Fudan University), Zhe Zhou (Fudan University), Zhou Li (University of California, Irvine)

**Mind the Gap: Studying the Insecurity of Provably Secure Embedded Trusted Execution Architectures**   
Marton Bognar (KU Leuven), Jo Van Bulck (KU Leuven), Frank Piessens (KU Leuven)

**Mitigating Information Leakage Vulnerabilities with Type-based Data Isolation**   
Alyssa Milburn (Vrije Universiteit Amsterdam, The Netherlands), Erik van der Kouwe (Vrije Universiteit Amsterdam, The Netherlands), Cristiano Giuffrida (Vrije Universiteit Amsterdam, The Netherlands)

**Model Orthogonalization: Class Distance Hardening in Neural Networks for Better Security**   
Guanhong Tao (Purdue University), Yingqi Liu (Purdue University), Guangyu Shen (Purdue University), Qiuling Xu (Purdue University), Shengwei An (Purdue University), Zhuo Zhang (Purdue University), Xiangyu Zhang (Purdue University)

**Model Stealing Attacks Against Inductive Graph Neural Networks**   
Yun Shen (Norton Research Group), Xinlei He (CISPA Helmholtz Center for Information Security), Yufei Han (Inria), Yang Zhang (CISPA Helmholtz Center for Information Security)

**Multi-Server Verifiable Computation of Low-Degree Polynomials**   
Liang Feng Zhang (ShanghaiTech University), Huaxiong Wang (Nanyang Technological University)

**Noise-SDR: Arbitrary Modulation of Electromagnetic Noise from Unprivileged Software and Its Impact on Emission Security**   
Giovanni Camurati (EURECOM, France), Aurélien Francillon (EURECOM, France)

**Noise: A Library of Verified High-Performance Secure Channel Protocol Implementations**   
Son Ho (INRIA), Jonathan Protzenko (Microsoft Research), Abhishek Bichhawat (IIT Gandhinagar), Karthikeyan Bhargavan (INRIA)

**PATA: Fuzzing with Path Aware Taint Analysis**   
Jie Liang (Tsinghua University, China), Mingzhe Wang (Tsinghua University, China), Chijin Zhou (Tsinghua University, China), Zhiyong Wu (Tsinghua University, China), Yu Jiang (Tsinghua University, China), (Jianzhong Liu (Tsinghua University, China), Zhe Liu (Nanjing University of Aeronautics and Astronautics, China), Jiaguang Sun (Tsinghua University, China)

**PCR-Auth: Solving Authentication Puzzle Challenges with Encoded Palm Contact Responses**   
Long Huang (Louisiana State University), Chen Wang (Louisiana State University)

**PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles**   
Hyungsub Kim (Purdue University), Muslum Ozgur Ozmen (Purdue University), Z. Berkay Celik (Purdue University), Antonio Bianchi (Purdue University), Dongyan Xu (Purdue University)

**PICCOLO: Exposing Complex Backdoors in NLP Transformer Models**   
Yingqi Liu (Purdue Univ.), Guangyu Shen (Purdue University), Guanhong Tao (Purdue University), Shengwei An (Purdue University), Shiqing Ma (Rutgers University), Xiangyu Zhang (Purdue University)

**PROTRR: Principled yet Optimal In-DRAM Target Row Refresh**   
Michele Marazzi (ETH Zurich), Patrick Jattke (ETH Zurich), Flavien Solt (ETH Zurich), Kaveh Razavi (ETH Zurich)

**Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes**   
Haojian Jin (Carnegie Mellon University), Gregory William Joseph Liu (Carnegie Mellon University), David Ethan Hwang (Carnegie Mellon University), Swarun Kumar (Carnegie Mellon University), Yuvraj Agarwal (Carnegie Mellon University), Jason Hong (Carnegie Mellon University)

**Phishing in Organizations: Findings from a Large-Scale and Long-Term Study**   
Daniele Lain (ETH Zurich), Kari Kostiainen (ETH Zurich), Srdjan Capkun (ETH Zurich)

**Practical Asynchronous Distributed Key Generation**   
Sourav Das (UIUC), Tom Yurek (UIUC), Zhuolun Xiang (UIUC), Andrew Miller (UIUC), Lefteris Kokoris-Kogias (IST Austria), Ling Ren (UIUC)

**Practical EMV Relay Protection**   
Andreea-Ina Radu (University of Birmingham, UK), Tom Chothia (University of Birmingham, UK), Christopher J.P. Newton (University of Surrey, UK), Ioana Boureanu (University of Surrey, UK), Liqun Chen (University of Surrey, UK)

**Privacy-from-Birth: Protecting Sensed Data from Malicious Sensors with VERSA**   
Ivan De Oliveira Nunes (Rochester Institute of Technology), Seoyeon Hwang (UC Irvine), Sashidhar Jakkamsetti (UC Irvine), Gene Tsudik (UC Irvine)

**Private Nearest Neighbor Search with Sublinear Communication and Malicious Security**   
Sacha Servan-Schreiber (Massachusetts Institute of Technology), Simon Langowski (Massachusetts Institute of Technology), Srinivas Devadas (Massachusetts Institute of Technology)

**ProVerif with Lemmas, Induction, Fast Subsumption, and Much More**   
Bruno Blanchet (Inria Paris), Vincent Cheval (Inria Paris), Véronique Cortier (Université de Lorraine, CNRS, Inria)

**Property Inference from Poisoning**   
Saeed Mahloujifar (Princeton), Esha Ghosh (Microsoft Research), Melissa Chase (Microsoft Research)

**Publicly Accountable Robust Multi-Party Computation**   
Marc Rivinius (University of Stuttgart), Pascal Reisert (University of Stuttgart), Daniel Rausch (University of Stuttgart), Ralf Küsters (University of Stuttgart)

**Quantifying Blockchain Extractable Value:How dark is the forest?**   
Kaihua Qin (Imperial College London), Liyi Zhou (Imperial College London), Arthur Gervais (Imperial College London)

**RT-TEE: Real-time System Availability for Cyber-physical Systems using ARM TrustZone**   
Jinwen Wang (Washington University in St. Louis), Ao Li (Washington University in St. Louis), Haoran Li (Washington University in St. Louis), Chenyang Lu (Washington University in St. Louis), Ning Zhang (Washington University in St. Louis)

**Reconstructing Training Data with Informed Adversaries**   
Borja Balle (DeepMind), Giovanni Cherubin (Alan Turing Institute), Jamie Hayes (DeepMind), Giovanni Cherubin (Alan Turing Institute)

**Repairing DoS Vulnerability of Real-World Regexes**   
Nariyoshi Chida (NTT Secure Platform Laboratories), Tachio Terauchi (Waseda University)

**Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms**   
Zhi Li (School of Cyber Science and Engineering, Huazhong University of Science and Technology, China; School of Computer Science and Technology, Huazhong University of Science and Technology, China; National Engineering Research Center for Big Data Technology and Sytem, China; Cluster and Grid Computing Lab, China; Services Computing Technology and System Lab, China; Big Data Security Engineering Research Center, China), Weijie Liu (Indiana University Bloomington, USA), Hongbo Chen (Indiana University Bloomington, USA), XiaoFeng Wang (Indiana University Bloomington, USA), Xiaojing Liao (Indiana University Bloomington, USA), Luyi Xing (Indiana University Bloomington, USA), Mingming Zha (Indiana University Bloomington, USA), Hai Jin (School of Computer Science and Technology, Huazhong University of Science and Technology, China; National Engineering Research Center for Big Data Technology and Sytem, China; Cluster and Grid Computing Lab, China; Services Computing, Deqing Zou (School of Cyber Science and Engineering, Huazhong University of Science and Technology, China; National Engineering Research Center for Big Data Technology and Sytem, China; Cluster and Grid Computing Lab, China; Services Computing Technology and System Lab, China; Big Data Security Engineering Research Center, China Technology and System Lab, China; Big Data Security Engineering Research Center, China)

**SAILFISH: Vetting Smart Contract State-Inconsistency Bugs in Seconds**   
Priyanka Bose (University of California, Santa Barbara), Dipanjan Das (University of California, Santa Barbara), Yanju Chen (University of California, Santa Barbara), Yu Feng (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (UC Santa Barbara)

**SIRAJ: A Unified Framework for Aggregation of Malicious Entity Detectors**   
Saravanan Thirumuruganathan (QCRI), Mohamed Nabeel (QCRI), Euijin Choo (Qatar Computing Research Institute), Issa Khalil (Qatar Computing Research Institute (QCRI), HBKU), Ting Yu (Qatar Computing Research Institute)

**SMILE: Secure Memory Introspection for Live Enclave**   
Lei Zhou (Southern University of Science and Technology (SUSTech)), Xuhua Ding (Singapore Management University), Fengwei Zhang (Southern University of Science and Technology (SUSTech))

**SNARKBlock: Federated Anonymous Blocklisting from Hidden Common Input Aggregate Proofs**   
Michael Rosenberg (University of Maryland), Mary Maller (Ethereum Foundation), Ian Miers (University of Maryland)

**SPURT: Scalable Distributed Randomness Beacon with Transparent Setup**   
Sourav Das (UIUC), Vinith Krishnan (UIUC), Irene Isaac (UIUC), Ling Ren (UIUC)

**SYMBEXCEL: Automated Analysis and Understanding of Malicious Excel 4.0 Macros**   
Nicola Ruaro (UC Santa Barbara), Fabio Pagani (UC Santa Barbara), Stefano Ortolani (VMware), Christopher Kruegel (UC Santa Barbara), Giovanni Vigna (UC Santa Barbara)

**Sabre: Sender-Anonymous Messaging with Fast Audits**   
Adithya Vadapalli (Indiana University Bloomington), Kyle Storrier (University of Calgary), Ryan Henry (University of Calgary)

**Scraping Sticky Leftovers: App User Information Left on Servers After Account Deletion**   
Preethi Santhanam (Wichita State University), Hoang Dang (Wichita State University), Zhiyong Shan (Wichita State University), Iulian Neamtiu (New Jersey Institute of Technology)

**SecFloat: Accurate Floating-Point meets Secure 2-Party Computation**   
Deevashwer Rathee (UC Berkeley), Anwesh Bhattacharya (Microsoft Research India), Rahul Sharma (Microsoft Research India), Divya Gupta (Microsoft Research India), Nishanth Chandran (Microsoft Research India), Aseem Rastogi (Microsoft Research India)

**Security Analysis of the MLS Key Derivation**   
Chris Brzuska (Aalto University, Finland), Eric Cornelissen (Aalto University, Finland), Konrad Kohbrok (Aalto University, Finland)

**Security Foundations for Application-Based Covert Communication Channels**   
James K Howes IV (University of Florida), Marios Georgiou (Galois), Alex Malozemoff (Galois), Thomas Shrimpton (University of Florida)

**ShadeWatcher: Recommendation-guided Cyber Threat Analysis using System Audit Records**   
Jun Zeng (National University of Singapore), Xiang Wang (National University of Singapore), Jiahao Liu (National University of Singapore), Yinfang Chen (University of Illinois - Urbana Champaign), Zhenkai Liang (National University of Singapore), Tat-Seng Chua (National University of Singapore), Zheng Leong Chua (Independent Researcher)

**ShorTor: Improving Tor Network Latency via Multi-hop Overlay Routing**   
Kyle Hogan (MIT), Sacha Servan-Schreiber (MIT), Zachary Newman (MIT), Ben Weintraub (Northeastern University), Cristina Nita-Rotaru (Northeastern University), Srinivas Devadas (MIT)

**SoK: A Framework for Unifying At-Risk User Research**   
Noel Warford (University of Maryland), Tara Matthews (Google), Kaitlyn Yang (University of Maryland), Omer Akgul (University of Maryland), Sunny Consolvo (Google), Patrick Gage Kelley (Google), Nathan Malkin (University of Maryland), Michelle L. Mazurek (University of Maryland), Manya Sleeper (Google), Kurt Thomas (Google)

**SoK: Authentication in Augmented and Virtual Reality**   
Sophie Stephenson (University of Wisconsin--Madison), Bijeeta Pal (Cornell University), Stephen Fan (University of Wisconsin--Madison), Earlence Fernandes (UW Madison), Yuhang Zhao (University of Wisconsin-Madison), Rahul Chatterjee (University of Wisconsin--Madison)

**SoK: Demystifying Binary Lifters Through the Lens of Downstream Applications**   
Zhibo Liu (The Hong Kong University of Science and Technology), Yuanyuan Yuan (The Hong Kong University of Science and Technology), Shuai Wang (The Hong Kong University of Science and Technology), Yuyan Bao (University of Waterloo)

**SoK: How Robust is Image Classification Deep Neural Network Watermarking?**   
Nils Lukas (University of Waterloo), Edward Jiang (University of Waterloo), Xinda Li (University of Waterloo), Florian Kerschbaum (University of Waterloo)

**SoK: Practical Foundations for Software Spectre Defenses**   
Sunjay Cauligi (UC San Diego), Craig Disselkoen (UC San Diego), Daniel Moghimi (UC San Diego), Gilles Barthe (MPI-SP and IMDEA Software Institute), Deian Stefan (UC San Diego)

**SoK: Social Cybersecurity**   
Yuxi Wu (Georgia Institute of Technology), W. Keith Edwards (Georgia Institute of Technology), Sauvik Das (Georgia Institute of Technology)

**SoK: The Dual Nature of Technology in Sexual Assault**   
Borke Obada-Obieh (The University of British Columbia), Yue Huang (University of British Columbia), Lucrezia Spagnolo (Vesta Social Innovation Technologies), Konstantin (Kosta) Beznosov (University of British Columbia)

**SpecHammer: Combining Spectre and Rowhammer for New Speculative Attacks**   
Youssef Tobah (The University of Michigan), Andrew Kwong (University of Michigan), Ingab Kang (University of Michigan), Daniel Genkin (Georgia Institute of Technology), Kang G. Shin (The University of Michigan)

**Sphinx: Enabling Privacy-Preserving Online Learning over the Cloud**   
Han Tian (Hong Kong University of Science and Technology), Chaoliang Zeng (Hong Kong University of Science and Technology), Zhenghang Ren (Hong Kong University of Science and Technology), Di Chai (Hong Kong University of Science and Technology), Junxue ZHANG (Hong Kong University of Science and Technology), Kai Chen (Hong Kong University of Science and Technology), Qiang Yang (Hong Kong University of Science and Technology)

**Spinning Language Models: Risks of Propaganda-as-a-Service and Countermeasures**   
Eugene Bagdasaryan (Cornell Tech), Vitaly Shmatikov (Cornell Tech)

**Spiral: Fast, High-Rate Single-Server PIR via FHE Composition**   
Samir Jordan Menon (None), David J. Wu (UT Austin)

**Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution**   
Ayush Agarwal (University of Michigan, USA), Sioli O’Connell (University of Adelaide, Australia), Jason Kim (Georgia Institute of Technology, USA), Shaked Yehezkel (Tel Aviv University, Israel), Daniel Genkin (Georgia Institute of Technology, USA), Eyal Ronen (Tel Aviv University, Israel), Yuval Yarom (University of Adelaide, Australia)

**Statistical Quantification of Differential Privacy: A Local Approach**   
Önder Askin (Ruhr-University Bochum), Tim Kutta (Ruhr-University Bochum), Holger Dette (Ruhr-University Bochum)

**Surakav: Generating Realistic Traces for a Strong Website Fingerprinting Defense**   
Jiajun GONG (The Hong Kong University of Science and Technology), Wuqi Zhang (The Hong Kong University of Science and Technology), Charles Zhang (The Hong Kong University of Science and Technology), Tao Wang (Simon Fraser University)

**SwarmFlawFinder: Discovering and Exploiting Logic Flaws of Swarm Algorithms**   
Chijung Jung (University of Virginia), Ali Ahad (University of Virginia), Yuseok Jeon (UNIST), Yonghwi Kwon (University of Virginia)

**TASHAROK: Using Mechanism Design for Enhancing Security Resource Allocation in Interdependent Systems**   
Mustafa Abdallah (Purdue University), Daniel Woods (University of Innsbruck), Parinaz Naghizadeh (Ohio State University), Issa Khalil (Qatar Computing Research Institute (QCRI), HBKU), Timothy Cason (Purdue University), Shreyas Sundaram (Purdue University), Saurabh Bagchi (Purdue University)

**TROLLMAGNIFIER: Detecting State-Sponsored Troll Accounts on Reddit?**   
Mohammad Hammas Saeed (Boston University), Shiza Ali (Boston University), Jeremy Blackburn (Binghamton University), Emiliano De Cristofaro (University College London), Savvas Zannettou (TU Delft), Gianluca Stringhini (Boston University)

**The State of the SameSite: Studying the Usage, Effectiveness, and Adequacy of SameSite Cookies**   
Soheil Khodayari (CISPA Helmholtz Center for Information Security, Germany), Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany)

**Time-Print: Authenticating USB Flash Drives with Novel Timing Fingerprints**   
Patrick Cronin (University of Delaware), Xing Gao (University of Delaware), Haining Wang (Virginia Tech), Chase Cotton (University of Delaware)

**Timing-Based Browsing Privacy Vulnerabilities Via Site Isolation**   
Zihao Jin (Microsoft Research Asia and Tsinghua University, China), Ziqiao Kong (Microsoft Research Asia, China), Shuo Chen (Microsoft Research Asia), Haixin Duan (Tsinghua University, China)

**Towards Automated Auditing for Account and Session Management Flaws in Single Sign-On Deployments**   
Mohammad Ghasemisharif (University of Illinois at Chicago), Chris Kanich (University of Illinois at Chicago), Jason Polakis (University of Illinois at Chicago)

**Transcending TRANSCEND: Revisiting Malware Classification in the Presence of Concept Drift**   
Federico Barbero (King's College London & University of Cambridge), Feargus Pendlebury (ICSI & King's College London & Royal Holloway, University of London), Fabio Pierazzi (King's College London), Lorenzo Cavallaro (University College London)

**Transfer Attacks Revisited: A Large-Scale Empirical Study in Real Computer Vision Settings**   
Yuhao Mao (Zhejiang University), Saizhuo Wang (Zhejiang University), Shouling Ji (Zhejiang University), Xuhong Zhang (Zhejiang University), Zhenguang Liu (Zhejiang Gongshang University), Jun Zhou (Ant Financial Services Group), Raheem Beyah (Georgia Institute of Technology), Ting Wang (Penn State)

**Universal 3-Dimensional Perturbations for Black-Box Attacks on Video Recognition Systems**   
Shangyu Xie (Illinois Institute of Technology, USA), Han Wang (Illinois Institute of Technology, USA), Yu Kong (Rochester Institute of Technology, USA), Yuan Hong (Illinois Institute of Technology, USA)

**Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains**   
Sri AravindaKrishnan Thyagarajan (Friedrich Alexander University of Erlangen-Nürnberg), Giulio Malavolta (Max Planck Institute for Security and Privacy), Pedro Moreno-Sanchez (IMDEA Software Institute)

**Using Throughput-Centric Byzantine Broadcast to Tolerate Malicious Majority in Blockchains**   
Ruomu Hou (National University of Singapore), Haifeng Yu (National University of Singapore), Prateek Saxena (National University of Singapore)

**WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens**   
Yan Jiang (Zhejiang University), Xiaoyu Ji (Zhejiang University), Kai Wang (Zhejiang University), Chen Yan (Zhejiang University), Richard Mitev (Technische University of Darmstadt), Ahmad-Reza Sadeghi (Technical University of Darmstadt), Wenyuan Xu (Zhejiang University)

**Waldo: A Private Time-Series Database from Function Secret-Sharing**   
Emma Dauterman (UC Berkeley), Mayank Rathee (UC Berkeley), Raluca Popa (UC Berkeley), Ion Stoica (UC Berkeley)

**Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques**   
Amit Seal Ami (William & Mary), Nathan Cooper (William & Mary), Kaushal Kafle (William & Mary), Kevin Moran (George Mason University), Denys Poshyvanyk (William & Mary), Adwait Nadkarni (William & Mary)

**Wobfuscator: Obfuscating JavaScript Malware via Opportunistic Translation to WebAssembly**   
Alan Romano (University at Buffalo, SUNY), Daniel Lehmann (University of Stuttgart), Michael Pradel (University of Stuttgart), Weihang Wang (University at Buffalo, SUNY)

**WtaGraph: Web Tracking and Advertising Detection using Graph Neural Networks**   
Zhiju Yang (Colorado School of Mines), Weiping Pei (Colorado School of Mines), Monchu Chen (Appen), Chuan Yue (Colorado School of Mines)

**ZeeStar: Private Smart Contracts by Homomorphic Encryption and Zero-knowledge Proofs**   
Samuel Steffen (ETH Zurich), Benjamin Bichsel (ETH Zurich), Roger Baumgartner (ETH Zurich), Martin Vechev (ETH Zurich)

**mmSpy: Spying Phone Calls using mmWave Radars**   
Suryoday Basak (Penn State University), Mahanth Gowda (Penn State University)

**vSGX: Virtualizing SGX Enclaves on AMD SEV**   
Shixuan Zhao (The Ohio State University), Mengyuan Li (The Ohio State University), Yinqian Zhang (Southern University of Science and Technology), Zhiqiang Lin (Ohio State University)

[](http://www.ieee.org/)[](http://www.computer.org/)[](http://www.ieee-security.org/)