**ACCEPTED PAPERS**

ACM CCS 2021 - November 15-19

**On the TOCTOU Problem in Remote Attestation**

*Ivan De Oliveira Nunes (UC Irvine); Sashidhar Jakkamsetti (UC Irvine); Norrathep Rattanavipanon (Prince of Songkla University); Gene Tsudik (UC Irvine)*

**Search-based Approaches for Local Black-Box Code Deobfuscation: Understand, Improve and Mitigate**

*Grégoire Menguy (CEA LIST); Sébastien Bardin (CEA LIST); Richard Bonichon (Nomadic Labs); Cauim de Souza Lima (CEA LIST)*

**Exorcising Spectres with Secure Compilers**

*Marco Patrignani (CISPA Helmholtz Center for Information Security & Stanford); Marco Guarnieri (IMDEA Software Institute)*

**Preventing Dynamic Library Compromise on Node.js via RWX-Based Privilege Reduction**

*Nikos Vasilakis (MIT); Cristian-Alexandru Staicu (CISPA Helmholtz Center for Information Security); Grigoris Ntousakis (TU Crete); Konstantinos Kallas (University of Pennsylvania); Ben Karel (Aarno Labs); Andre DeHon (University of Pennsylvania); Michael Pradel (University of Stuttgart)*

**Consistency Analysis of Data-Usage Purposes in Mobile Apps**

*Duc Bui (University of Michigan); Yuan Yao (University of Michigan); Kang G. Shin (The University of Michigan); Jong-Min Choi (Samsung Research); Junbum Shin (CryptoLab)*

**C3PO: Large-Scale Study Of Covert Monitoring of C&C Servers via Over-Permissioned Protocol Infiltration**

*Jonathan Fuller (Georgia Institute of Technology); Ranjita Pai Kasturi (Georgia Institute of Technology); Amit Sikder (Georgia Institute of Technology); Haichuan Xu (Georgia Institute of Technology); Berat Arik (Georgia Institute of Technology); Vivek Verma (Georgia Institute of Technology); Ehsan Asdar (Georgia Institute of Technology); Brendan Saltaformaggio (Georgia Institute of Technology)*

**Cert-RNN: Towards Certifying the Robustness of Recurrent Neural Networks**

*Tianyu Du (Zhejiang University); Shouling Ji (Zhejiang University); Lujia Shen (Zhejiang University); Yao Zhang (Zhejiang University); Jinfeng Li (Zhejiang University); Jie Shi (Huawei International, Singapore); Chengfang Fang (Huawei International, Singapore); Jianwei Yin (Zhejiang University); Raheem Beyah (Georgia Institute of Technology); Ting Wang (Pennsylvania State University)*

**Secure Source-Tracking for Encrypted Messaging**

*Charlotte Peale (Stanford University); Saba Eskandarian (Stanford University); Dan Boneh (Stanford University)*

**LEAP: Leakage-Abuse Attack on Efficiently Deployable, Efficiently Searchable Encryption with Partially Known Dataset**

*Jianting Ning (Fujian Normal University & Singapore Management University); Xinyi Huang (Fujian Normal University); Geong Sen Poh (NUS-Singtel Cyber Security Research and Development Laboratory); Jiaming Yuan (Singapore Management University); Yingjiu Li (University of Oregon); Jian Weng (Jinan University); Robert H. Deng (School of Information Systems, Singapore Management University, Singapore)*

**AHEAD: Adaptive Hierarchical Decomposition for Range Query under Local Differential Privacy**

*Linkang Du (Zhejiang University); Zhikun Zhang (CISPA Helmholtz Center for Information Security); Shaojie Bai (Zhejiang University); Changchang Liu (IBM Research); Shouling Ji (Zhejiang University); Peng Cheng (Zhejiang University); Jiming Chen (Zhejiang University)*

**Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees**

*Matthew Weidner (Carnegie Mellon University); Martin Kleppmann (University of Cambridge); Daniel Hugenroth (University of Cambridge); Alastair R. Beresford (University of Cambridge)*

**SNIPUZZ: Black-box Fuzzing of IoT Firmware via Message Snippet Inference**

*Xiaotao Feng (Swinburne University of Technology); Ruoxi Sun (The University of Adelaide); Xiaogang Zhu (Swinburne University of Technology); Minhui Xue (The University of Adelaide); Sheng Wen (Swinburne University of Technology); Dongxi Liu (Data61, CSIRO); Surya Nepal (Data61 CSIRO Australia); Yang Xiang (Swinburne University of Technology)*

**Unleashing the Tiger: Inference Attacks on Split Learning**

*Dario Pasquini (Sapienza University of Rome; Institute of Applied Computing, IAC-CNR); Giuseppe Ateniese (Stevens Institute of Technology); Massimo Bernaschi (Institute of Applied Computing, IAC-CNR)*

**Fuzzy Message Detection**

*Gabrielle Beck (Johns Hopkins University); Julia Len (Cornell Tech); Ian Miers (University of Maryland); Matthew Green (Johns Hopkins University)*

**Dissecting Click Fraud Autonomy in the Wild**

*Tong Zhu (Shanghai Jiao Tong University); Yan Meng (Shanghai Jiao Tong University); Haotian Hu (Shanghai Jiao Tong University); Xiaokuan Zhang (The Ohio State University); Minhui Xue (The University of Adelaide); Haojin Zhu (Shanghai Jiao Tong University)*

**Understanding and Detecting Mobile Ad Fraud Through the Lens of Invalid Traffic**

*Suibin Sun (Shanghai Jiao Tong University); Le Yu (Shanghai Jiao Tong University); Xiaokuan Zhang (The Ohio State University); Minhui (Jason) Xue (The University of Adelaide); Ren Zhou (Shanghai Jiao Tong University); Haojin Zhu (Shanghai Jiao Tong University); Shuang Hao (University of Texas at Dallas); Xiaodong Lin (University of Guelph)*

**Mechanized Proofs of Adversarial Complexity and Application to Universal Composability**

*Manuel Barbosa (University of Porto (FCUP) and INESC TEC); Gilles Barthe (MPI-SP and IMDEA Software Institute); Benjamin Grégoire (INRIA Sophia Antipolis); Adrien Koutsos (INRIA Paris); Pierre-Yves Strub (Ecole Polytechnique)*

**Periscope: A Keystroke Inference Attack Using Human Coupled Electromagnetic Emanations**

*Wenqiang Jin (The University of Texas at Arlington); Srinivasan Murali (The University of Texas at Arlington); Huadi Zhu (The University of Texas at Arlington); Ming Li (The University of Texas at Arlington)*

**Meteor: Cryptographically Secure Steganography for RealisticDistributions**

*Gabriel Kaptchuk (Boston University); Tushar Jois (Johns Hopkins University); Matthew Green (Johns Hopkins University); Aviel Rubin (Johns Hopkins University)*

**TableGAN-MCA: Evaluating Membership Collisions of GAN-Synthesized Tabular Data Releasing**

*Aoting Hu (Southeast University); Renjie Xie (Southeast University); Zhigang Lu (Macquarie University); Aiqun Hu (Southeast University); Minhui Xue (The University of Adelaide)*

**"I need a better description": An Investigation Into User Expectations For Differential Privacy**

*Rachel Cummings (Columbia University); Gabriel Kaptchuk (Boston University); Elissa M. Redmiles (Max Planck Institute for Software Systems)*

**Usable User Authentication on a Smartwatch using Vibration**

*Sunwoo Lee (Korea University); Wonsuk Choi (Hansung University); Dong Hoon Lee (Korea University)*

**Multi-Threshold Byzantine Fault Tolerance**

*Atsuki Momose (Nagoya University); Ling Ren (University of Illinois at Urbana-Champaign)*

**Verifying Table-Based Elections**

*David Basin (Institute of Information Security, Department of Computer Science, ETH Zurich); Jannik Dreier (Universite de Lorraine, CNRS, Inria, LORIA); Sofia Giampietro (Institute of Information Security, Department of Computer Science, ETH Zurich); Sasa Radomirovic (Department of Computer Science, Heriot-Watt University)*

**QuickSilver: Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field**

*Kang Yang (State Key Laboratory of Cryptology); Pratik Sarkar (Boston University); Chenkai Weng (Northwestern University); Xiao Wang (Northwestern University)*

**Secure Multi-party Computation of Differentially Private Heavy Hitters**

*Jonas Böhler (SAP Security Research); Florian Kerschbaum (University of Waterloo)*

**ZKCPlus: Optimized Fair-exchange Protocol Supporting Practical and Flexible Data Exchange**

*Yun Li (Institute for Network Sciences and Cyberspace of Tsinghua University); Cun Ye (SECBIT Labs, kecheng corp); Yuguang Hu (SECBIT Labs); Ivring Morpheus (SECBIT Labs); Guo Yu (SECBIT Labs); Chao Zhang (Institute for Network Science and Cyberspace of Tsinghua University); Yupeng Zhang (Texas A&M University); Zhipeng Sun (SECBIT Labs); Yiwen Lu (SECBIT Labs); Haodi Wang (Beijing Normal University)*

**It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications**

*Qingying Hao (University of Illinois at Urbana-Champaign); Licheng Luo (University of Illinois at Urbana-Champaign); Steve TK Jan (University of Illinois at Urbana-Champaign); Gang Wang (University of Illinois at Urbana-Champaign)*

**Secure Graph Analysis at Scale**

*Toshinori Araki (NEC); Jun Furukawa (NEC Israel Research Center); Benny Pinkas (VMware Research, Bar Ilan University); Kazuma Ohara (AIST); Hanan Rosemarin (Bar Ilan University); Hikaru Tsuchida (NEC corporation)*

**Revisiting Nakamoto Consensus in Asynchronous Networks: A Comprehensive Analysis of Bitcoin Safety and Chain Quality**

*Muhammad Saad (University of Central Florida); Afsah Anwar (University of Central Florida); Srivatsan Ravi (University of Southern California); David Mohaisen (University of Central Florida)*

**PPE Circuits for Rational Polynomials**

*Susan Hohenberger (Johns Hopkins University); Satyanarayana Vusirikala (University of Texas at Austin)*

**PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild**

*Daniel De Almeida Braga (Univ Rennes 1, CNRS, IRISA); Pierre-Alain Fouque (Univ Rennes 1, CNRS, IRISA); Mohamed Sabt (Univ Rennes 1, CNRS, IRISA)*

**CROSSLINE: Breaking ``Security-by-Crash'' based Memory Isolation in AMD SEV**

*Mengyuan Li (The Ohio State University); Yinqian Zhang (Southern University of Science and Technology); Zhiqiang Lin (The Ohio State University)*

**Locally Private Graph Neural Networks**

*Sina Sajadmanesh (Idiap Research Institute, EPFL); Daniel Gatica-Perez (Idiap Research Institute, EPFL)*

**BFT Protocol Forensics**

*Peiyao Sheng (University of Illinois at Urbana-Champaign); Gerui Wang (UIUC); Kartik Nayak (Duke University); Sreeram Kannan (University of Washington); Pramod Viswanath (UIUC)*

**Securing Parallel-chain Protocols under Variable Mining Power**

*Xuechao Wang (University of Illinois Urbana-Champaign); Viswa Virinchi Muppirala (University of Washington at Seattle); Lei Yang (MIT CSAIL); Sreeram Kannan (University of Washington at Seattle); Pramod Viswanath (University of Illinois Urbana-Champaign)*

**A One-Pass Distributed and Private Sketch for Kernel Sums with Applications to Machine Learning at Scale**

*Benjamin Coleman (Rice University); Anshumali Shrivastava (Rice University)*

**All your credentials are belong to us: On Insecure WPA2-Enterprise Configurations**

*Man Hong Hue (The Chinese University of Hong Kong); Joyanta Debnath (The University of Iowa); Kin Man Leung (The University of British Columbia); Li Li (Syracuse University); Mohsen Minaei (Visa Research); M. Hammad Mazhar (The University of Iowa); Kailiang Xian (The Chinese University of Hong Kong); Endadul Hoque (Syracuse University); Omar Chowdhury (The University of Iowa); Sze Yiu Chau (The Chinese University of Hong Kong)*

**On the Robustness of Domain Constraints**

*Ryan Sheatsley (The Pennsylvania State University); Blaine Hoak (The Pennsylvania State University); Eric Pauley (The Pennsylvania State University); Yohan Beugin (The Pennsylvania State University); Michael J. Weisman (United States Army Research Laboratory); Patrick McDaniel (The Pennsylvania State University)*

**Amortized Threshold Symmetric-key Encryption**

*Pratyay Mukherjee (Visa Research); Rohit Sinha (Swirlds Inc.); Sivanarayana Gaddam (C3 Inc.); Mihai Christodorescu (Visa Research)*

**Shorter and Faster Post-Quantum zkSNARKs from Lattices**

*Yuval Ishai (Technion); Hang Su (University of Virginia); David J. Wu (University of Virginia)*

**Hardware Support to Improve Fuzzing Performance and Precision**

*Ren Ding (Georgia Institute of Technology); Yonghae Kim (Georgia Institute of Technology); Fan Sang (Georgia Institute of Technology); Wen Xu (Georgia Institute of Technology); Gururaj Saileshwar (Georgia Institute of Technology); Taesoo Kim (Georgia Institute of Technology)*

**RandPiper -- Reconfiguration-Friendly Random Beacons with Quadratic Communication**

*Adithya Bhat (Purdue University); Nibesh Shrestha (Rochester Institute of Technology); Zhongtang Luo (Purdue University); Aniket Kate (Purdue University); Kartik Nayak (Duke University)*

**Membership Leakage in Label-Only Exposures**

*Zheng Li (CISPA Helmholtz Center for Information Security); Yang Zhang (CISPA Helmholtz Center for Information Security)*

**Hidden Backdoors in Human-Centric Language Models**

*Shaofeng Li (Shanghai Jiao Tong University); Hui Liu (Shanghai Jiao Tong University); Tian Dong (Shanghai Jiao Tong University); Benjamin Zi Hao Zhao (The University of New South Wales and CSIRO-Data61); Minhui Xue (The University of Adelaide); Haojin Zhu (Shanghai Jiao Tong University); Jialiang Lu (Shanghai Jiao Tong University)*

**Spinner: Automated Dynamic Command Subsystem Perturbation**

*Meng Wang (University of Virginia); Chijung Jung (University of Virginia); Ali Ahad (University of Virginia); Yonghwi Kwon (University of Virginia)*

**SugarCoat: Programmatically Generating Privacy-Preserving, Web-Compatible Resource Replacements for Content Blocking**

*Michael Smith (University of California, San Diego); Peter Snyder (Brave Software); Benjamin Livshits (Brave Software, Imperial College London); Deian Stefan (University of California, San Diego)*

**DataLens: Scalable Privacy Preserving Training via Gradient Compression and Aggregation**

*Boxin Wang (University of Illinois at Urbana-Champaign); Fan Wu (UIUC); Yunhui Long (University of Illinois at Urbana-Champaign); Luka Rimanic (ETH Zurich); Ce Zhang (ETH Zurich); Bo Li (UIUC)*

**On-device IoT Certificate Revocation Checking with Small Memory and Low Latency**

*Xiaofeng Shi (University of California, Santa Cruz); Shouqian Shi (University of California, Santa Cruz); Minmei Wang (University of California, Santa Cruz); Jonne Kaunisto (University of California, Santa Cruz); Chen Qian (University of California, Santa Cruz)*

**MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets**

*Tohid Shekari (Georgia Institute of Technology); Celine Irvene (Georgia Institute of Technology); Alvaro Cardenas (UC Santa Cruz); Raheem Beyah (Georgia Institute of Technology)*

**With a Little Help from My Friends: Constructing Practical Anonymous Credentials**

*Lucjan Hanzlik (CISPA Helmholtz Center for Information Security); Daniel Slamanig (AIT Austrian Institute of Technology)*

**Constantine: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization**

*Pietro Borrello (Sapienza University of Rome); Daniele Cono D'Elia (Sapienza University of Rome); Leonardo Querzoni (Sapienza University of Rome); Cristiano Giuffrida (Vrije Universiteit Amsterdam)*

**Oblivious Linear Group Actions and Applications**

*Nuttapong Attrapadung (AIST, Japan); Goichiro Hanaoaka (AIST, Japan); Takahiro Matsuda (AIST, Japan); Hiraku Morita (University of St. Gallen, Switzerland); Kazuma Ohara (AIST, Japan); Jacob Schuldt (AIST, Japan); Tadanori Teruya (AIST, Japan); Kazunari Tozawa (University of Tokyo, Japan)*

**Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis**

*Chuanpu Fu (Tsinghua University); Qi Li (Tsinghua University); Meng Shen (Beijing Institute of Technology); Ke Xu (Tsinghua University)*

**Revisiting Fuzzy Signatures: Towards a More Risk-Free Cryptographic Authentication System based on Biometrics**

*Shuichi Katsumata (AIST); Takahiro Matsuda (AIST); Wataru Nakamura (Hitachi, Ltd.) Kazuma Ohara (AIST); Kenta Takahashi (Hitachi, Ltd.);*

**PalmTree: Learning an Assembly Language Model for Instruction Embedding**

*Xuezixiang Li (University of California Riverside); Yu Qu (University of California Riverside); Heng Yin (University of California Riverside)*

**TSS: Transformation-Specific Smoothing for Robustness Certification**

*Linyi Li (University of Illinois at Urbana-Champaign); Maurice Weber (ETH Zürich); Xiaojun Xu (University of Illinois at Urbana-Champaign); Luka Rimanic (ETH Zürich); Bhavya Kailkhura (Lawrence Livermore National Laboratory); Tao Xie (Peking University); Ce Zhang (ETH Zürich); Bo Li (University of Illinois at Urbana-Champaign)*

**DeepAID: Interpreting and Improving Deep Learning-based Anomaly Detection in Security Applications**

*Dongqi Han (Tsinghua University); Zhiliang Wang (Tsinghua University); Wenqi Chen (Tsinghua University); Ying Zhong (Tsinghua university); Su Wang (Tsinghua University); Han Zhang (Tsinghua University); Jiahai Yang (Tsinghua University); Xingang Shi (Tsinghua University); Xia Yin (Tsinghua University)*

**Hiding the Lengths of Encrypted Messages via Gaussian Padding**

*Jean Paul Degabriele (TU Darmstadt)*

**Efficient Linear Multiparty PSI and Extensions to Circuit/Quorum PSI**

*Nishanth Chandran (Microsoft Research, Bangalore); Nishka Dasgupta (Microsoft Research, Bangalore); Divya Gupta (Microsoft Research, Bangalore); Sai Lakshmi Bhavana Obbattu (Microsoft Research, Bangalore); Sruthi Sekar (Indian Institute of Science, Bangalore); Akash Shah (Microsoft Research, Bangalore)*

**On the (in)security of ElGamal in OpenPGP**

*Luca De Feo (IBM Research - Zurich); Bertram Poettering (IBM Research - Zurich); Alessandro Sorniotti (IBM Research - Zurich)*

**Locating the Security Patches for Disclosed OSS Vulnerabilities with Vulnerability-Commit Correlation Ranking**

*Xin Tan (Fudan University); Yuan Zhang (Fudan University); Chenyuan Mi (Fudan University); Jiajun Cao (Fudan University); Kun Sun (George Mason University); Yifan Lin (Fudan University); Min Yang (Fudan University)*

**Facilitating Vulnerability Assessment through PoC Migration**

*Jiarun Dai (Fudan University); Yuan Zhang (Fudan University); Hailong Xu (Fudan University); Haiming Lyu (Fudan University); Zicheng Wu (Fudan University); Xinyu Xing (Pennsylvania State University); Min Yang (Fudan University)*

**Efficient Zero-knowledge MPCitH-based Arguments**

*Cyprien Delpech de Saint Guilhem (KU Leuven); Emmanuela Orsini (KU Leuven); Titouan Tanguy (KU Leuven)*

**Regression Greybox Fuzzing**

*Xiaogang Zhu (Swinburne University of Technology); Marcel Böhme (Monash University)*

**Honest-but-Curious Nets: Sensitive Attributes of Private Inputs Can Be Secretly Coded into the Classifiers' Outputs**

*Mohammad Malekzadeh (Imperial College London); Anastasia Borovykh (Imperial College London); Deniz Gunduz (Imperial College London)*

**Wireless Charging Power Side-Channel Attacks**

*Alexander La Cour (Cornell University); Edward Suh (Cornell University); Khurram Afridi (Cornell University)*

**A Security Framework for Distributed Ledgers**

*Christoph Egger (Friedrich-Alexander University Erlangen-Nürnberg); Mike Graf (University of Stuttgart); Ralf Küsters (University of Stuttgart); Daniel Rausch (University of Stuttgart); Viktoria Ronge (Friedrich-Alexander University Erlangen-Nürnberg); Dominique Schröder (Friedrich-Alexander University Erlangen-Nürnberg)*

**Differential Privacy for Directional Data**

*Benjamin Weggenmann (SAP SE); Florian Kerschbaum (University of Waterloo)*

**Automated Bug Hunting With Data-Driven Symbolic Root Cause Analysis**

*Carter Yagemann (Georgia Institute of Technology); Simon P. Chung (Georgia Institute of Technology); Brendan Saltaformaggio (Georgia Institute of Technology); Wenke Lee (Georgia Institute of Technology)*

**Differentially private sparse vectors with low error, optimal space, and fast access**

*Martin Aumüller (IT University of Copenhagen); Christian Janos Lebeda (BARC and IT University of Copenhagen); Rasmus Pagh (BARC and University of Copenhagen)*

**Supply-Chain Vulnerability Elimination via Active Learning and Regeneration**

*Nikos Vasilakis (MIT); Achilles Benetopoulos (UC Santa Cruz); Shivam Handa (MIT); Alizee Schoen (MIT); Jiasi Shen (MIT); Martin Rinard (MIT)*

**Deterrence of Intelligent DDoS via Multi-Hop Traffic Divergence**

*Yuanjie Li (Tsinghua University); Hewu Li (Tsinghua University); Zhizheng Lv (Tsinghua University); Xingkun Yao (Tsinghua University); Qianru Li (University of California, Los Angeles); Jianping Wu (Tsinghua University)*

**Igor: Crash Deduplication Through Root-Cause Clustering**

*Zhiyuan Jiang (National University of Defense Technology); Xiyue Jiang (National University of Defense Technology); Ahmad Hazimeh (EPFL); Chaojing Tang (National University of Defense Technology); Chao Zhang (Tsinghua University); Mathias Payer (EPFL)*

**CPscan: Detecting Bugs Caused by Code Pruning in IoT Kernels**

*Lirong Fu (Zhejiang University); Shouling Ji (Zhejiang University); Kangjie Lu (University of Minnesota); Peiyu Liu (Zhejiang University); Xuhong Zhang (Zhejiang University); Yuxuan Duan (Zhejiang University); Zihui Zhang (Zhejiang University); Wenzhi Chen (Zhejiang University); Yanjun Wu (Institute of Software, Chinese Academy of Sciences)*

**XSinator.com: From a Formal Model to the Automatic Evaluation of Cross-Site Leaks in Web Browsers**

*Lukas Knittel (Ruhr University Bochum); Christian Mainka (Ruhr University Bochum); Marcus Niemietz (Ruhr University Bochum); Dominik Trevor Noß (Ruhr University Bochum); Jörg Schwenk (Ruhr University Bochum)*

**HardsHeap: A Universal and Extensible Framework for Evaluating Secure Allocators**

*Insu Yun (KAIST); Woosun Song (KAIST); Seunggi Min (KAIST); Taesoo Kim (Georgia Institute of Technology)*

**The Invisible Shadow: How Security Cameras Leak Private Activities**

*Jian Gong (Central South University); Xinyu Zhang (University of California, San Diego); Ju Ren (Central South University); Yaoxue Zhang (Tsinghua University)*

**"Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World**

*Emily Wenger (University of Chicago); Max Bronckers (University of Chicago); Christian Cianfarani (University of Chicago); Jenna Cryan (University of Chicago); Angela Sha (University of Chicago); Haitao Zheng (University of Chicago); Ben Y. Zhao (University of Chicago)*

**Chunk-Level Password Guessing: Towards Modeling Refined Password Composition Representations**

*Ming Xu (Fudan University); Chuanwang Wang (Fudan University); Jitao Yu (Fudan University); Junjie Zhang (Fudan University); Kai Zhang (Fudan University); Weili Han (Fudan University)*

**MirChecker: Detecting Bugs in Rust Programs via Static Analysis**

*Zhuohua Li (The Chinese University of Hong Kong); Jincheng Wang (The Chinese University of Hong Kong); Mingshen Sun (Baidu Security); John C.S. Lui (The Chinese University of Hong Kong)*

**Demons in the Shared Kernel: Abstract Resource Attacks Against OS-level Virtualization**

*Nanzi Yang (Xidian University); Wenbo Shen (Zhejiang University); Jinku Li (Xidian University); Yutian Yang (Zhejiang University); Kangjie Lu (University of Minnesota); Jietao Xiao (Xidian University); Tianyu Zhou (Zhejiang University); Chenggang Qin (Ant Group); Wang Yu (Ant Group); Jianfeng Ma (Xidian University); Kui Ren (Zhejiang University)*

**FakeWake: Understanding and Mitigating Fake Wake-up Words of Voice Assistants**

*Yanjiao Chen (Zhejiang University); Yijie Bai (Zhejiang University); Kaibo Wang (Zhejiang University); Richard Mitev (Technische Universität Darmstadt); Wenyuan Xu (Zhejiang University); Ahmad-Reza Sadeghi (Technische Universität Darmstadt)*

**Towards Transparent and Stealthy Android OS Sandboxing via Customizable Container-Based Virtualization**

*Wenna Song (Wuhan University); Jiang Ming (University of Texas at Arlington); Lin Jiang (XDJA); Yi Xiang (Wuhan University); Xuanchen Pan (Wuhan Antiy Information Technology); Jianming Fu (Wuhan University); Guojun Peng (Wuhan University)*

**DoubleX: Statically Analyzing Browser Extensions at Scale**

*Aurore Fass (CISPA Helmholtz Center for Information Security); Dolière Francis Somé (CISPA Helmholtz Center for Information Security); Michael Backes (CISPA Helmholtz Center for Information Security); Ben Stock (CISPA Helmholtz Center for Information Security)*

**Biometrics-Authenticated Key Exchange for Secure Messaging**

*Mei Wang (Wuhan University); Kun He (Wuhan University); Jing Chen (Wuhan University); Zengpeng Li (Shandong University); Wei Zhao (Science and Technology on Communication Security Laboratory); Ruiying Du (Wuhan University)*

**Validating the Integrity of Audit Logs Against Execution Repartitioning Attacks**

*Carter Yagemann (Georgia Institute of Technology); Mohammad Noureddine (University of Illinois Urbana-Champaign); Wajih Ul Hassan (University of Illinois Urbana-Champaign); Simon Chung (Georgia Institute of Technology); Adam Bates (University of Illinois Urbana-Champaign); Wenke Lee (Georgia Institute of Technology)*

**Reconstructing with Less: Leakage Abuse Attacks in Two-Dimensions**

*Evangelia Anna Markatou (Brown University); Francesca Falzon (University of Chicago); Roberto Tamassia (Brown University); William Schor (Brown University)*

**This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration**

*Michalis Diamantaris (FORTH); Serafeim Moustakas (FORTH); Lichao Sun (Lehigh University); Sotiris Ioannidis (Technical University of Crete); Jason Polakis (University of Illinois at Chicago)*

**Scan, Test, Execute: Adversarial Tactics in Amplification DDoS Attacks**

*Harm Griffioen (Hasso Plattner Institute); Kris Oosthoek (Delft University of Technology); Paul van der Knaap (Delft University of Technology); Christian Doerr (Hasso Plattner Institute)*

**Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale**

*Stijn Pletinckx (TU Delft); Kevin Borgolte (Ruhr University Bochum); Tobias Fiebig (TU Delft)*

**HyperFuzzer: An Efficient Hybrid Fuzzer For Virtual CPUs**

*Xinyang Ge (Microsoft Research); Ben Niu (Microsoft); Robert Brotzman (The Pennsylvania State University); Yaohui Chen (Facebook); HyungSeok Han (KAIST); Patrice Godefroid (Microsoft Research); Weidong Cui (Microsoft Research)*

**EncoderMI: Membership Inference against Pre-trained Encoders in Contrastive Learning**

*Hongbin Liu (Duke University); Jinyuan Jia (Duke University); Wenjie Qu (Huazhong University of Science and Technology); Neil Gong (Duke University)*

**Subpopulation Data Poisoning Attacks**

*Matthew Jagielski (Northeastern University); Giorgio Severi (Northeastern University); Niklas Pousette Harger (Northeastern University); Alina Oprea (Northeastern University)*

**Continuous Release of Data Streams under both Centralized and Local Differential Privacy**

*Tianhao Wang (Purdue University); Joann Qiongna Chen (University of California, Irvine); Zhikun Zhang (CISPA Helmholtz Center for Information Security); Dong Su (Alibaba); Yueqiang Cheng (NIO Security Research); Zhou Li (University of California, Irvine); Ninghui Li (Purdue University); Somesh Jha (University of Wisconsin)*

**Side-channel attacks on query-based data anonymization**

*Franziska Boenisch (Fraunhofer AISEC); Reinhard Munz (Max Planck Institute for Software Systems (MPI-SWS)); Marcel Tiepelt (Karlsruhe Institute of Technology); Simon Hanisch (Karlsruhe Institute of Technology); Christiane Kuhn (Karlsruhe Institute of Technology); Paul Francis (Max Planck Institute for Software Systems (MPI-SWS))*

**How Does Blockchain Security Dictate Blockchain Implementation?**

*Andrew Lewis-Pye (London School of Economics); Tim Roughgarden (Columbia University)*

**ECMO: Peripheral Transplantation to Rehost Embedded Linux Kernels**

*Muhui Jiang (The Hong Kong Polytechnic University; Zhejiang University); Lin Ma (Zhejiang University); Yajin Zhou (Zhejiang University); Qiang Liu (Zhejiang University); Cen Zhang (Nanyang Technological University); Zhi Wang (Florida State University); Xiapu Luo (The Hong Kong Polytechnic University); Lei Wu (Zhejiang University); Kui Ren (Zhejiang University)*

**The return of Eratosthenes: Secure Generation of RSA Moduli using Distributed Sieving**

*Cyprien Delpech de Saint Guilhem (imec-COSIC, KU Leuven, Belgium); Eleftheria Makri (imec-COSIC, KU Leuven, Belgium; ABRR, Saxion University of Applied Sciences, The Netherlands); Dragos Rotaru (Cape Privacy; imec-COSIC, KU Leuven, Belgium); Titouan Tanguy (imec-COSIC, KU Leuven, Belgium)*

**Robust Detection of Machine-induced Audio Attacks in Intelligent Audio Systems with Microphone Array**

*Zhuohang Li (University of Tennessee, Knoxville); Cong Shi (Rutgers University); Tianfang Zhang (Rutgers University); Yi Xie (Rutgers University); Jian Liu (University of Tennessee, Knoxville); Bo Yuan (Rutgers University); Yingying Chen (Rutgers University)*

**When Machine Unlearning Jeopardizes Privacy**

*Min Chen (CISPA Helmholtz Center for Information Security); Zhikun Zhang (CISPA Helmholtz Center for Information Security); Tianhao Wang (Purdue University); Michael Backes (CISPA Helmholtz Center for Information Security); Mathias Humbert (Cyber-Defence Campus, armasuisse S+T); Yang Zhang (CISPA Helmholtz Center for Information Security)*

**DetectorGuard: Provably Securing Object Detectors against Localized Patch Hiding Attacks**

*Chong Xiang (Princeton University); Prateek Mittal (Princeton University)*

**New Directions in Automated Traffic Analysis**

*Jordan Holland (Princeton University); Paul Schmitt (Princeton University); Nick Feamster (University of Chicago); Prateek Mittal (Princeton University)*

**An Inside Look into the Practice of Malware Analysis**

*Miuyin Yong Wong (Georgia Institute of Technology); Matthew Landen (Georgia Institute of Technology); Manos Antonakakis (Georgia Tech); Douglas M. Blough (Georgia Institute of Technology); Elissa M. Redmiles (Max Planck Institute for Software Systems); Mustaque Ahamad (Georgia Tech)*

**Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication**

*Kelong Cong (imec-COSIC, KU Leuven); Radames Cruz Moreno (Microsoft Research); Mariana Botelho da Gama (imec-COSIC, KU Leuven); Wei Dai (Microsoft Research); Ilia Iliashenko (imec-COSIC, KU Leuven); Kim Laine (Microsoft Research); Michael Rosenberg (University of Maryland)*

**DETER: Denial of Ethereum Txpool sERvices**

*Kai Li (Syracuse University); Yibo Wang (Syracuse University); Yuzhe Tang (Syracuse University)*

**Structured Leakage and Applications to Cryptographic Constant-Time and Cost**

*Gilles Barthe (MPI-SP, IMDEA Software Institute); Benjamin Grégoire (Université Côte d’Azur, Inria, Sophia Antipolis); Vincent Laporte (Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France); Swarn Priya (Université Côte d’Azur, Inria, Sophia Antipolis)*

**Themis: Ambiguity-Aware Network Intrusion Detection based on Symbolic Model Comparison**

*Zhongjie Wang (University of California, Riverside); Shitong Zhu (University of California, Riverside); Keyu Man (University of California, Riverside); Pengxiong Zhu (University of California, Riverside); Yu Hao (University of California, Riverside); Zhiyun Qian (University of California, Riverside); Srikanth V. Krishnamurthy (University of California, Riverside); Tom La Porta (Pennsylvania State University); Michael J. De Lucia (U.S. Army Research Laboratory)*

**SyzGen: Automated Generation of Syscall Specification of Closed-Source macOS Drivers**

*Weiteng Chen (UC Riverside); Yu Wang (Didi Research America); Zheng Zhang (UC Riverside); Zhiyun Qian (UC Riverside)*

**The Effect of Google Search on Software Security**

*Felix Fischer (Professorship of Cyber Trust, Department of Informatics, Technical University Munich); Yannick Stachelscheid (Professorship of Cyber Trust, Department of Informatics, Technical University Munich); Jens Grossklags (Professorship of Cyber Trust, Department of Informatics, Technical University Munich)*

**One Hot Garbling**

*David Heath (Georgia Institute of Technology); Vladimir Kolesnikov (Georgia Institute of Technology)*

**DNS Cache Poisoning Attack: Resurrections with Side Channels**

*Keyu Man (University of California, Riverside); Xinan Zhou (University of California, Riverside); Zhiyun Qian (University of California, Riverside)*

**Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits**

*Brian Kondracki (Stony Brook University); Babak Amin Azad (Stony Brook University); Oleksii Starov (Palo Alto Networks); Nick Nikiforakis (Stony Brook University)*

**I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights**

*Wei Wang (University of Maryland, Baltimore County); Yao Yao (University of Maryland, Baltimore County); Xin Liu (University of Maryland, Baltimore County); Xiang Li (Independent Researcher); Pei Hao (University of Maryland, Baltimore County); Ting Zhu (University of Maryland, Baltimore County)*

**EasyPQC: Verifying Post-Quantum Cryptography**

*Manuel Barbosa (University of Porto (FCUP) and INESC TEC); Gilles Barthe (MPI-SP and IMDEA Software Institute); Xiong Fan (University of Maryland); Benjamin Grégoire (Inria); Shih-Han Hung (University of Maryland); Jonathan Katz (University of Maryland); Pierre-Yves Strub (École Polytechnique); Xiaodi Wu (University of Maryland); Li Zhou (MPI-SP)*

**SyncAttack: Double-spending in Bitcoin Without Mining Power**

*Muhammad Saad (University of Central Florida); Songqing Chen (George Mason University); David Mohaisen (University of Central Florida)*

**Backdoor Pre-trained Models Can Transfer to All**

*Lujia Shen (Zhejiang University); Shouling Ji (Zhejiang University); Xuhong Zhang (Zhejiang University); Jinfeng Li (Zhejiang University); Jing Chen (Wuhan University); Jie Shi (Huawei International, Singapore); Chengfang Fang (Huawei International, Singapore); Jianwei Yin (Zhejiang University); Ting Wang (Penn State)*

**Packet scheduling with optional client privacy**

*Andrew Beams (University of Pennsylvania); Sampath Kannan (University of Pennsylvania); Sebastian Angel (University of Pennsylvania)*

**Warmonger: Inflicting Denial-of-Service via Serverless Functions in the Cloud**

*Junjie Xiong (University of South Florida); Mingkui Wei (George Mason University); Zhuo Lu (University of South Florida); Yao Liu (University of South Florida)*

**Quantifying and Mitigating Privacy Risks of Contrastive Learning**

*Xinlei He (CISPA Helmholtz Center for Information Security); Yang Zhang (CISPA Helmholtz Center for Information Security)*

**Doubly Efficient Interactive Proofs for General Arithmetic Circuits with Linear Prover Time**

*Jiaheng Zhang (UC Berkeley); Tianyi Liu (Texas A&M University & Shanghai Key Laboratory of Privacy-Preserving Computation); Weijie Wang (Shanghai Jiao Tong University); Yinuo Zhang (UC Berkeley); Dawn Song (UC Berkeley); Xiang Xie (Shanghai Key Laboratory of Privacy-Preserving Computation); Yupeng Zhang (Texas A&M University)*

**Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem**

*Yiming Zhang (Tsinghua University); Baojun Liu (Tsinghua University); Chaoyi Lu (Tsinghua University; 360 Netlab); Zhou Li (University of California, Irvine); Haixin Duan (Tsinghua University; QI-ANXIN Technology Research Institute; Beijing National Research Center for Information Science and Technology; Peng Cheng Laboratory); Jiachen Li (Tsinghua University); Zaifeng Zhang (360 Netlab)*

**Indistinguishability Prevents Scheduler Side-Channels in Real-Time Systems**

*Chien-Ying Chen (University of Illinois at Urbana-Champaign); Debopam Sanyal (University of Illinois at Urbana-Champaign); Sibin Mohan (University of Illinois at Urbana-Champaign)*

**Detecting Missed Security Operations Through Differential Checking of Object-based Similar Paths**

*Dinghao Liu (Zhejiang University); Qiushi Wu (University of Minnesota); Shouling Ji (Zhejiang University); Kangjie Lu (University of Minnesota); Zhenguang Liu (Zhejiang University); Jianhai Chen (Zhejiang University); Qinming He (Zhejiang University)*

**Membership Inference Attacks Against Recommender Systems**

*Minxing Zhang (Shandong University); Zihan Wang (Shandong University); Yang Zhang (CISPA Helmholtz Center for Information Security); Zhaochun Ren (Shandong University); Pengjie Ren (Shandong University); Zhunmin Chen (Shandong University); Pengfei Hu (Shandong University)*

**Machine-checked ZKP for NP relations: Formally Verified Security Proofs and Implementations of MPC-in-the-Head**

*José Bacelar Almeida (University of Minho and INESC TEC); Manuel Barbosa (University of Porto (FCUP) and INESC TEC); Manuel L Correia (University of Porto (FCUP) and INESC TEC); Karim Eldefrawy (SRI International); Stéphane Graham-Lengrand (SRI International); Hugo Pacheco (University of Porto (FCUP) and INESC TEC); Vitor Pereira (SRI International)*

**An In-Depth Symbolic Security Analysis of the ACME Standard**

*Karthikeyan Bhargavan (INRIA Paris, France); Abhishek Bichhawat (IIT Gandhinagar, India); Quoc Huy Do (University of Stuttgart, Germany and GLIWA GmbH, Germany); Pedram Hosseyni (University of Stuttgart, Germany); Ralf Küsters (University of Stuttgart, Germany); Guido Schmitz (University of Stuttgart, Germany); Tim Würtele (University of Stuttgart, Germany)*

**Who's In Control? On Security Risks of Disjointed IoT Device Management Channels**

*Yan Jia (Nankai University); Bin Yuan (Huazhong University of Science and Technology); Luyi Xing (Indiana University Bloomington); Dongfang Zhao (Indiana University Bloomington); XiaoFeng Wang (Indiana University Bloomington); Yifan Zhang (Indiana University Bloomington); Yijing Liu (Nankai University); Kaimin Zheng (Huazhong University of Science and Technology); Peyton Crnjak (Indiana University Bloomington); Yuqing Zhang (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences); Deqing Zou (Huazhong University of Science and Technology); Hai Jin (Huazhong University of Science and Technology)*

**Simple, Fast Malicious Multiparty Private Set Intersection**

*Ofri Nevo (Open University of Israel); Ni Trieu (Arizona State University); Avishay Yanai (VMware Research)*

**Efficient CCA Timed Commitments in Class Groups**

*Guilhem Castagnos (University of Bordeaux); Fabien Laguillaumie (Université of Montpellier); Giulio Malavolta (Max Planck Institute for Security and Privacy); Sri Aravinda Krishnan Thyagarajan (Friedrich-Alexander University of Erlangen-Nuremberg)*

**Android on PC: On the Security of End-user Android Emulators**

*Fenghao Xu (The Chinese University of Hong Kong); Siyu Shen (The Chinese University of Hong Kong); Wenrui Diao (Shandong University); Zhou Li (University of California, Irvine); Yi Chen (The Chinese University of Hong Kong); Rui Li (Shandong University); Kehuan Zhang (The Chinese University of Hong Kong)*

**Glowworm Attack: Optical TEMPEST Sound Recovery via a Device’s Power Indicator LED**

*Ben Nassi (Ben-Gurion University of the Negev); Yaron Pirutin (Ben-Gurion University of the Negev); Tomer Galor (Ben-Gurion University of the Negev); Yuval Elovici (Ben-Gurion University of the Negev); Boris Zadov (Ben-Gurion University of the Negev)*

**Learning Security Classifiers with Verified Global Robustness Properties**

*Yizheng Chen (Columbia University); Shiqi Wang (Columbia University); Yue Qin (Indiana University Bloomington); Xiaojing Liao (Indiana University Bloomington); Suman Jana (Columbia University); David Wagner (UC Berkeley)*

**Robust Adversarial Attacks Against DNN-Based Wireless Communication Systems**

*Alireza Bahramali (UMASS Amherst); Milad Nasr (UMASS Amherst); Amir Houmansadr (UMass Amherst); Dennis Goeckel (UMASS Amherst); Don Towsley (University of Massachusetts - Amherst)*

**Compact and Malicious Private Set Intersection for Small Sets**

*Mike Rosulek (Oregon State University); Ni Trieu (Arizona State University)*

**One Glitch to Rule Them All: Fault Injection Attacks Against AMD’s Secure Encrypted Virtualization**

*Robert Buhren (Technische Universität Berlin); Hans-Niklas Jacob (Technische Universität Berlin); Thilo Krachenfels (Technische Universität Berlin); Jean-Pierre Seifert (Technische Universität Berlin)*

**12 Angry Developers – A Qualitative Study on Developers’ Struggles with CSP**

*Sebastian Roth (CISPA Helmholtz Center for Information Security); Lea Theresa Gröber (CISPA Helmholtz Center for Information Security); Michael Backes (CISPA Helmholtz Center for Information Security); Katharina Krombholz (CISPA Helmholtz Center for Information Security); Ben Stock (CISPA Helmholtz Center for Information Security)*

**DPGen: Automated Program Synthesis for Differential Privacy**

*Yuxin Wang (Pennsylvania State University); Zeyu Ding (Pennsylvania State University); Yingtai Xiao (Pennsylvania State University); Daniel Kifer (Pennsylvania State University); Danfeng Zhang (Pennsylvania State University)*

**Aion: Enabling Open Systems through Strong Availability Guarantees for Enclaves**

*Fritz Alder (KU Leuven); Jo Van Bulck (KU Leuven); Frank Piessens (KU Leuven); Jan Tobias Mühlberg (KU Leuven)*

**Util::Lookup: Exploiting key decoding in cryptographic libraries**

*Florian Sieck (University of Lübeck); Sebastian Berndt (University of Lübeck); Jan Wichelmann (University of Lübeck); Thomas Eisenbarth (University of Lübeck)*

**Mining in Logarithmic Space**

*Aggelos Kiayias (University of Edinburgh and IOHK); Nikos Leonardos (University of Athens); Dionysis Zindros (University of Athens)*

**Dissecting Residual APIs in Custom Android ROMs**

*Zeinab El-Rewini (University of Waterloo); Yousra Aafer (University of Waterloo)*

**MPC-Friendly Commitments for Publicly Verifiable Covert Security**

*Nitin Agrawal (University of Oxford); James Bell (The Alan Turing Institute); Adria Gascon (Google LLC); Matt Kusner (University College London, The Alan Turing Institute)*

**A formally verified configuration for Hardware Security Modules in the cloud**

*Riccardo Focardi (University Ca' Foscari, Venice and Cryptosense); Flaminia L. Luccio (University Ca' Foscari, Venice)*

**VIP: Safeguard Value Invariant Property for Thwarting Critical Memory Corruption Attacks**

*Mohannad Ismail (Virginia Tech); Jinwoo Yom (Virginia Tech); Christopher Jelesnianski (Virginia Tech); Yeongjin Jang (Oregon State University); Changwoo Min (Virginia Tech)*

**Epsolute: Efficiently Querying Databases While Providing Differential Privacy**

*Dmytro Bogatov (Boston University); Georgios Kellaris (Boston University); George Kollios (Boston University); Kobbi Nissim (Georgetown University); Adam O'Neill (University of Massachusetts, Amherst)*

**Same Coverage, Less Bloat: Accelerating Binary-only Fuzzing with Coverage-preserving Coverage-guided Tracing**

*Stefan Nagy (Virginia Tech); Anh Nguyen-Tuong (University of Virginia); Jason Hiser (University of Virginia); Jack Davidson (University of Virginia); Matthew Hicks (Virginia Tech)*

**RealSWATT: Remote Software-based Attestation for Embedded Devices under Realtime Constraints**

*Sebastian Surminski (University of Duisburg-Essen); Christian Niesler (University of Duisburg-Essen); Ferdinand Brasser (TU Darmstadt); Lucas Davi (University of Duisburg-Essen); Ahmad-Reza Sadeghi (TU Darmstadt)*

**Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?**

*Yi Zhu (University at Buffalo, the State University at New York); Chenglin Miao (University of Georgia); Tianhang Zheng (University of Toronto); Foad Hajiaghajani (University at Buffalo, the State University at New York); Lu Su (Purdue University); Chunming Qiao (SUNY at Buffalo)*

**DroneKey: A Drone-Aided Group-Key Generation Scheme for Large-Scale IoT Networks**

*Dianqi Han (Arizona State University); Ang Li (Arizona State University); Jiawei Li (Arizona State University); Yan Zhang (Arizona State University); Tao Li (Indiana University–Purdue University Indianapolis); Yanchao Zhang (Arizona State University)*

**The One-Page Setting: A Higher Standard for Evaluating Website Fingerprinting Defenses**

*Tao Wang (Simon Fraser University)*

**Don't Forget the Stuffing! Revisiting the Security Impact of Typo-Tolerant Password**

*Sena Sahin (Georgia Institute of Technology); Frank Li (Georgia Institute of Technology)*

**Compressed Oblivious Encoding for Homomorphically Encrypted Search**

*Seung Geol Choi (US Naval Academy); Dana Dachman-Soled (University of Maryland, College Park); S. Dov Gordon (George Mason University); Linsheng Liu (George Washington University); Arkady Yerukhimovich (George Washington University)*

**Feature Indistinguishable Attack to Circumvent Trapdoor-enabled Defense**

*Chaoxiang He (Huazhong University of Science and Technology); Bin (Benjamin) Zhu (Microsoft Research Asia); Xiaojing Ma (Huazhong University of Science and Technology); Hai Jin (Huazhong University of Science and Technology); Shengshan Hu (Huazhong University of Science and Technology)*

**On Reengineering the X.509 PKI with Executable Specification for Better Implementation Guarantees**

*Joyanta Debnath (The University of Iowa); Sze Yiu Chau (The Chinese University of Hong Kong); Omar Chowdhury (The University of Iowa)*

**On the Renyi Differential Privacy of the Shuffle Model**

*Antonious M. Girgis (University of California Los Angeles, USA); Deepesh Data (University of California Los Angeles, USA); Suhas Diggavi (University of California Los Angeles, USA); Ananda Suresh (Google Research); Peter Kairouz (Google Research)*

**Zero Knowledge Static Program Analysis**

*Zhiyong Fang (Texas A&M University); David Darais (Galois, Inc); Joe Near (University of Vermont); Yupeng Zhang (Texas A&M University)*

**A Hard Label Black-box Adversarial Attack Against Graph Neural Networks**

*Jiaming Mu (Tsinghua University); Binghui Wang (Duke University); Qi Li (Tsinghua University); Kun Sun (George Mason University); Mingwei Xu (Tsinghua University); Zhuotao Liu (Tsinghua University)*

**COINN: Crypto/ML Codesign for Oblivious Inference via Neural Networks**

*Siam U. Hussain (University of California San Diego); Mojan Javaheripi (University of California San Diego); Mohammad Samragh (University of California San Diego); Farinaz Koushanfar (University of California San Diego)*

**Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels**

*Hang Zhang (University of California, Riverside); Weiteng Chen (University of California, Riverside); Yu Hao (University of California, Riverside); Guoren Li (University of California, Riverside); Yizhuo Zhai (University of California, Riverside); Xiaochen Zou (University of California, Riverside); Zhiyun Qian (University of California, Riverside)*

**WristPrint: Characterizing User Re-identification Risks from Wrist-worn Accelerometry Data**

*Nazir Saleheen (University of Memphis); Md Azim Ullah (University of Memphis); Supriyo Chakraborty (IBM T. J. Watson Research Center); Deniz Ones (University of Minnesota); Mani Srivastava (University of California, Los Angeles); Santosh Kumar (University of Memphis)*

**Constant-Overhead Zero-Knowledge for RAM Programs**

*Nicholas Franzese (Northwestern University); Jonathan Katz (University of Maryland); Steve Lu (Stealth Software Technologies, Inc.); Rafail Ostrovsky (UCLA); Xiao Wang (Northwestern University); Chenkai Weng (Northwestern University)*

**Ghost in the Binder: Binder Transaction Redirection Attacks in Android System Services**

*Xiaobo Xiang (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Ren Zhang (Nervos); Hanxiang Wen (Ant Group); Xiaorui Gong (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Baoxu Liu (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences)*

**Generalized Proof of Liabilities**

*Yan Ji (Cornell University); Konstantinos Chalkias (Novi / Facebook)*

**Efficient Online-friendly Two-Party ECDSA Signature**

*Haiyang Xue (The University of Hong Kong,); Man Ho Au (The University of Hong Kong); Xiang Xie (Shanghai Key Laboratory of Privacy-Preserving Computation); Tsz Hon Yuen (The University of Hong Kong); Handong Cui (The University of Hong Kong)*

**APECS: A Distributed Access Control Framework for Pervasive Edge Computing Services**

*Sean Dougherty (Saint Louis University); Reza Tourani (Saint Louis University); Gaurav Panwar (New Mexico State University); Roopa Vishwanathan (New Mexico State University); Satyajayant Misra (New Mexico State University); Srikathyayani Srikanteswara (Intel Corp.)*

**Reverse Attack: Black-box Attacks on Collaborative Recommendation**

*Yihe Zhang (University of Louisiana at Lafayette); Xu Yuan (University of Louisiana at Lafayette); Jin Li (Guangzhou University, China); Jiadong Lou (University of Louisiana at Lafayette); Li Chen (University of Louisiana at Lafayette); Nianfeng Tzeng (University of Louisiana at Lafayette)*

**zkCNN: Zero Knowledge Proofs for Convolutional Neural Network Predictions and Accuracy**

*Tianyi Liu (Texas A&M University & Shanghai Key Laboratory of Privacy-Preserving Computation); Xiang Xie (Shanghai Key Laboratory of Privacy-Preserving Computation); Yupeng Zhang (Texas A&M University)*

**A PKI-based Framework for Establishing Efficient MPC Channels**

*Daniel Masny (Visa Research); Gaven Watson (Visa Research)*

**The Exact Security of BIP32 Wallets**

*Poulami Das (Technische Universität Darmstadt); Andreas Erwig (Technische Universität Darmstadt); Sebastian Faust (Technische Universität Darmstadt); Julian Loss (University of Maryland); Siavash Riahi (Technische Universität Darmstadt)*

**Asynchronous Data Dissemination and its Applications**

*Sourav Das (UIUC); Zhuolun Xiang (UIUC); Ling Ren (UIUC)*

**OpenSquare: Decentralized Repeated Modular Squaring Service**

*Sri Aravinda Krishnan Thyagarajan (Friedrich-Alexander University of Erlangen-Nuremberg); Adithya Bhat (Purdue University); Tiantian Gong (Purdue University); Aniket Kate (Purdue University); Dominique Schröder (Friedrich-Alexander Universität Erlangen-Nürnberg)*

**Rosita++: Automatic Higher-Order Leakage Elimination from Cryptographic Code**

*Madura Shelton (University of Adelaide); Łukasz Chmielewski (University of Radboud and Riscure); Niels Samwel (Radboud University); Markus Wagner (University of Adelaide); Lejla Batina (Radboud University); Yuval Yarom (University of Adelaide)*

**OnionPIR: Response Efficient Single-Server PIR**

*Muhammad Haris Mughees (University of Illinois at Urbana-Champaign); Hao Chen (Facebook, USA); Ling Ren (University of Illinois at Urbana-Champaign);*

**Morpheus: Bringing The (PKCS) One To Meet the Oracle**

*Moosa Yahyazadeh (The University of Iowa); Sze Yiu Chau (The Chinese University of Hong Kong); Li Li (Syracuse University); Man Hong Hue (The Chinese University of Hong Kong); Joyanta Debnath (The University of Iowa); Sheung Chiu Ip (The Chinese University of Hong Kong); Li Chun Ngai (The Chinese University of Hong Kong); Endadul Hoque (Syracuse University); Omar Chowdhury (The University of Iowa)*

**Black-box Adversarial Attacks on Commercial Speech Platforms with Minimal Information**

*Baolin Zheng (Wuhan University); Peipei Jiang (Wuhan University); Qian Wang (Wuhan University); Qi Li (Tsinghua University); Chao Shen (Xi'an Jiaotong University); Cong Wang (City University of Hong Kong); Yunjie Ge (Wuhan University); Qingyang Teng (Wuhan University); Shenyi Zhang (Wuhan University)*

**Solver-Aided Constant-Time Hardware Verification**

*Rami Gökhan Kıcı (University of California, San Diego); Klaus v. Gleissenthall (Vrije Universiteit Amsterdam); Deian Stefan (University of California, San Diego); Ranjit Jhala (University of California, San Diego)*

**V-SHUTTLE: Scalable and Semantics-Aware Hypervisor Fuzzing**

*Gaoning Pan (Zhejiang University & Ant Group); Xingwei Lin (Ant Group); Xuhong Zhang (Zhejiang University); Yongkang Jia (Zhejiang University); Shouling Ji (Zhejiang University); Chunming Wu (Zhejiang University); Xinlei Ying (Ant Group); Jiashui Wang (Ant Group); Yanjun Wu (Institute of Software, Chinese Academy of Sciences)*

**T-Reqs: HTTP Request Smuggling with Differential Fuzzing**

*Bahruz Jabiyev (Northeastern University); Steven Sprecher (Northeastern University); Kaan Onarlioglu (Akamai Technologies); Engin Kirda (Northeastern University)*

**United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale**

*Daniel Wagner (DE-CIX/MPI-INF); Daniel Kopp (DE-CIX); Matthias Wichtlhuber (DE-CIX); Christoph Dietzel (DE-CIX/MPI-INF); Oliver Hohlfeld (Brandenburg University of Technology); Georgios Smaragdakis (TU Delft); Anja Feldmann (MPI-INF)*

**Appenzeller to Brie: Efficient Zero-Knowledge Proofs for Mixed-Mode Arithmetic and $\Z\_{2^k}$**

*Carsten Baum (Aarhus University); Lennart Braun (Aarhus University); Alexander Munch-Hansen (Aarhus University); Peter Scholl (Aarhus University)*

**Learning to Explore Paths for Symbolic Execution**

*Jingxuan He (ETH Zurich); Gishor Sivanrupan (ETH Zurich); Petar Tsankov (ETH Zurich); Martin Vechev (ETH Zurich)*

**You Make Me Tremble: A First Look at Attacks Against Structural Control Systems**

*Abel Zambrano (Universidad de los Andes); Alejandro Palacio Betancur (Penn State University); Luis Burbano (University of California, Santa Cruz); Andres Felipe Niño (Universidad de los Andes); Luis Felipe Giraldo (Universidad de los Andes); Mariantonieta Gutierrez Soto (Penn State University); Jairo Giraldo (University of Utah); Alvaro A. Cardenas (University of California, Santa Cruz)*

**Structural Attack against Graph Based Android Malware Detection**

*Kaifa Zhao (The Hong Kong Polytechnic University); Hao Zhou (The Hong Kong Polytechnic University); Yulin Zhu (The Hong Kong Polytechnic University); Xian Zhan (The Hong Kong Polytechnic University); Kai Zhou (The Hong Kong Polytechnic University); Jianfeng Li (The Hong Kong Polytechnic University); Le Yu (The Hong Kong Polytechnic University); Wei Yuan (Huazhong University of Science and Technology); Xiapu Luo (The Hong Kong Polytechnic University)*

**The Security of ChaCha20-Poly1305 in the Multi-User Setting**

*Jean Paul Degabriele (TU Darmstadt); Jérôme Govinden (TU Darmstadt); Felix Günther (ETH Zurich); Kenny Paterson (ETH Zurich)*

**Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices**

*Syed Rafiul Hussain (Pennsylvania State University); Imtiaz Karim (Purdue University); Abdullah Al Ishtiaq (Pennsylvania State University); Omar Chowdhury (The University of Iowa); Elisa Bertino (Purdue University)*

**Let's Downgrade Let's Encrypt**

*Tianxiang Dai (ATHENE Center & Fraunhofer SIT); Haya Shulman (ATHENE Center & Fraunhofer SIT); Michael Waidner (ATHENE Center & TU Darmstadt & Fraunhofer SIT)*

**Prime+Scope: Overcoming the Observer Effect for High-Precision Cache Contention Attacks**

*Antoon Purnal (imec-COSIC, KU Leuven); Furkan Turan (imec-COSIC, KU Leuven); Ingrid Verbauwhede (imec-COSIC, KU Leuven)*

**CapSpeaker: Injecting Sounds to Microphones via Capacitors**

*Xiaoyu Ji (Zhejiang University); Juchuan Zhang (Zhejiang University); Shui Jiang (Zhejiang University); Jishen Li (Zhejiang University); Wenyuan Xu (Zhejiang University)*

**A Concrete Treatment of Efficient Continuous Group Key Agreement via Multi-Recipient PKEs**

*Keitaro Hashimoto (Tokyo Institute of Technology and AIST, Japan); Shuichi Katsumata (AIST, Japan); Eamonn W. Postlethwaite (Royal Holloway, University of London, Egham, UK); Thomas Prest (PQShield Ltd., UK); Bas Westerbaan (PQShield Ltd., UK)*

**AI-Lancet: Locating Error-inducing Neurons to Optimize Neural Networks**

*Yue Zhao (SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China); Hong Zhu (SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China); Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences, China); Shengzhi Zhang (Department of Computer Science, Metropolitan College, Boston University, USA)*

**Faster Lattice-Based KEMs via a Generic Fujisaki-Okamoto Transform Using Prefix Hashing**

*Julien Duman (Ruhr-Universität Bochum); Kathrin Hövelmanns (Eindhoven University of Technology); Eike Kiltz (Ruhr-Universität Bochum); Vadim Lyubashevsky (IBM Research Europe, Zurich); Gregor Seiler (IBM Research Europe, Zurich, ETH Zurich)*

**Modular Design of Secure Group Messaging Protocols and the Security of MLS**

*Yiannis Tselekounis (University of Edinburgh); Sandro Coretti (IOHK); Joël Alwen (Wickr); Yevgeniy Dodis (New York University)*

**SmashEx: Smashing SGX Enclaves Using Exceptions**

*Jinhua Cui (National University of Defense Technology, National University of Singapore); Zhijingcheng Yu (National University of Singapore); Shweta Shinde (ETH Zurich); Prateek Saxena (National University of Singapore); Zhiping Cai (National University of Defense Technology)*

**Private Hierarchical Clustering in Federated Networks**

*Aashish Kolluri (National University Of Singapore); Teodora Baluta (National University of Singapore); Prateek Saxena (National University of Singapore)*

**SoFi: Reflection-Augmented Fuzzing for JavaScript Engines**

*Xiaoyu He (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Xiaofei Xie (Nanyang Technological University); Yuekang Li (Nanyang Technological University); Jianwen Sun (Nanyang Technological University); Feng Li (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Wei Zou (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Yang Liu (Nanyang Technological University); Lei Yu (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Jianhua Zhou (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Wenchang Shi (Renmin University of China); Wei Huo (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences)*