November 15–19, 2021
Virtual Event, Republic of Korea

Association for
Computing Machinery

Advancing Computing as a Science & Profession

CCS '21

Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

General Chairs:

Yongdae Kim, KAIST, Republic of Korea
Jong Kim, POSTECH, Republic of Korea

Program Chairs:

Giovanni Vigna, University of California, Santa Barbara / VMware, USA
Elaine Shi, Carnegie Mellon University, USA

Publication Chairs:

Hyoungshick Kim, Sungkyunkwan University, Republic of Korea
Jin B. Hong, University of Western Australia, Australia

Association for
Computing Machinery

Advancing Computing as a Science & Profession

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

Copyright © 2021 by the Association for Computing Machinery, Inc. (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from: permissions@acm.org or Fax +1 (212) 869-0481.

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

ISBN: 978-1-4503-8454-4

Additional copies may be ordered prepaid from:

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

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

Printed in the USA

Message from the ACM CCS 2021 General Co-Chairs

On behalf of the ACM CCS 2021 Organizing Committee, we welcome you to the 27th ACM Annual Conference on Computer and Communication Security (CCS). ACM CCS continues to be the premier Security conference, where researchers, practitioners, and educators come together to present, discuss, and debate the most recent research results, innovations, trends, and concerns in the field of Computer and Communication Security.

This is the first time ACM CCS has been set to occur in South Korea. South Korea is a particularly appropriate location for ACM CCS: it is a country that has embraced technology and currently has the 12th largest economy in the world. At the same time, it is a country in which the old and new co-exist: e.g., traditional Korean music and K-pop, traditional Korean cuisine and Western foods, Oscar-winning movies, and pansori storytelling.

ACM CCS 2021 was originally scheduled to take place in person. Unfortunately, due to the ongoing COVID-19 crisis, we have decided to change the format of the conference to be fully virtual. We feel deep sorrow about not being able to have all of you in Seoul, South Korea.

This year's main CCS conference will be one of the largest with over 190 paper presentations in three days. This year, we are trying a new conference format since it is virtual. All presentation videos are available in advance, and we will have a live discussion with the authors in each session. The main conference is scheduled to occur in conjunction with numerous workshops. We are also glad to have three distinguished keynote speakers for the CCS conference: Dr. Cynthia Dwork (Harvard University, USA), Dr. Dawn Song (UC Berkeley, USA), and Dr. Taesoo Kim (Georgia Tech., USA and Samsung Research, Korea) will present their keynotes at the first session on each day during the main conference.

We are immensely grateful to the members of the Organizing Committee—a team of volunteers drawn from South Korea and around the world—who have contributed a tremendous amount of time and effort over a year into making the conference a success. We are particularly thankful to the Program Chairs, Giovanni Vigna and Elaine Shi, the Track Chairs, and all Program Committee members for selecting the content of the technical track itself, and we are additionally thankful to Giovanni and Elaine for overseeing the structure and integrity of the entire main program. We are thankful to our Workshop Chairs (Michael Franz and Dokyung Song), all chairs of our co-located workshops for overseeing the assemblage of our partner events, and the members of their respective program committees -- all together, they have contributed to an exceptional collection of conference programming and events. We owe a special debt of gratitude to our organization committee members: Web Chairs (Byoungyoung Lee), Publications Chairs (Hyoungshick Kim and Jin B. Hong), Treasurer (Changhoon Lee), Registrations Chair (Jongsung Kim), Publicity Chairs (Yeongjin Jang and Insu Yun), Organizational Chair (Jin Kwak), Poster Chair (Esha Ghosh), Student Grant Chairs (Doowon Kim and Yonghwi Kwon), and Sponsorship Chairs (Kyoung Ho Lee, David Mohaisen, and Kui Ren). Their devotion made this conference possible.

Beyond all of the foregoing individuals, there are several organizations to which we are deeply beholden. We thank ACM and its Special Interest Group on Security, Audit and Control (SIGSAC) and the Korea Institute of Information Security & Cryptology (KIISC) for their sponsorship of ACM CCS 2021. We are also deeply grateful to our corporate sponsors for their generous support. As of this writing, those sponsors include Huawei, the National Science Foundation (NSF), VMware, ANT Financial Group, Baidu, Facebook, Samsung Research, Ahn Lab, Google, Naver, Technology Innovation Institute (TII), and IOHK.

Finally, thank you to all of the authors and other contributors for your involvement with ACM CCS. You are the reason CCS is the premier conference in Computer and Communications Security.

Sincerely,

ACM CCS 2021 General Chairs!

Yongdae Kim
KAIST

Jong Kim
POSTECH

Program Chairs' Welcome

Last year these remarks opened by hoping that the 2020 edition of the ACM CCS conference would be both the first and the last to be held virtually. Unfortunately, this is not the case. Once again, ACM CCS will be held virtually, due to the persisting COVID-19 pandemic. This has created challenges especially for our amazing General Chairs, who had to navigate the uncertainty of the times leading to the final decision of keeping the conference virtual and then devise novel ways to support participation and interaction within the ACM CCS community.

The task of the Program Committee, led by the Program Chairs and the Track Chairs, was to select the papers that would appear in this edition of the conference. Keeping with the tradition, we had two reviewing cycles, with submission deadlines in January and May, each with a roughly 2.5-month review cycle. Due to the large number of papers submitted, and to give to the authors the opportunity to submit their papers elsewhere, some papers were rejected early in the process, as the result of receiving two negative reviews. For the remaining papers, authors were given the opportunity to engage in an interactive rebuttal to address specific concerns of the reviewers. By the end of each cycle, each submitted paper was marked for acceptance, conditional acceptance (shepherding), rejection, or revision. Papers in the last category were allowed to be resubmitted for another round of review, under the assumption that they would be accepted if the requirements set by the reviewers (in some cases requiring extensive work) were met satisfactorily.

All submissions were reviewed by a Program Committee of 235 security and privacy experts from around the world, along with many expert sub-reviewers from outside the committee. The Program Co-Chairs were assisted by ten Track Chairs (Herbert Bos, Adam Doupe, Phillipa Gill, Limin Jia, Sarah Meiklejohn, Jelena Mirkovic, Prateek Saxena, Jonathan Ullman, Muthuramakrishnan Venkitasubramaniam, and Wenyuan Xu) who are recognized experts in their respective subfields. The Track Chairs were also involved in selecting the award papers.

The January cycle received 315 submissions, with 43 papers accepted (possibly with shepherding). An additional 30 papers were chosen for revision, with 22 of those eventually being accepted after the revised version was submitted. Of the papers that were rejected, 94 were rejected early. A total of 565 papers were submitted to the May cycle, with 84 papers accepted (possibly with shepherding) and 63 papers chosen to be revised. From the latter group, 47 papers were eventually accepted. Of the rejected papers, 168 were rejected early. Altogether, 196 out of 879 submissions were accepted, for an acceptance rate of 22%.

The accepted papers cover a wide range of topics in security, including web security, machine learning, network security, formal methods, software security, IoT/CPS security, applied cryptography, privacy and anonymity, security usability and measurement, and blockchain security.

We thank the Track Chairs, PC members, and external reviewers for their contributions to the conference and for their dedication to reviewing under challenging circumstances. We are also extremely grateful to the General Chairs, Yongdae Kim and Jong Kim, for organizing the virtual conference.

We also thank all the authors for submitting their work to ACM CCS.

We hope you enjoy the conference!

Giovanni Vigna
University of California, Santa Barbara/VMware

Elaine Shi
Carnegie Mellon University

Table of Contents

ACM CCS 2021 Conference Organization xxiii

ACM CCS 2021 Sponsor & Supporters xxx

Keynote Talks

- **Pseudo-Randomness and the Crystal Ball** 1
  Cynthia Dwork *(Harvard University)*
- **Towards Building a Responsible Data Economy** 3
  Dawn Song *(University of California, Berkeley)*
- **Are we done yet? Our Journey to Fight against Memory-safety Bugs** 4
  Taesoo Kim *(Georgia Institute of Technology & Samsung Research)*

Session 1A: Cybercrime

- **Chunk-Level Password Guessing: Towards Modeling Refined Password Composition Representations** 5
  Ming Xu, Chuanwang Wang, Jitao Yu, Junjie Zhang, Kai Zhang, Weili Han *(Fudan University)*
- **Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale** 21
  Stijn Pletinckx *(TU Delft)*, Kevin Borgolte *(Ruhr University Bochum)*,
  Tobias Fiebig *(TU Delft)*
- **Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits** 36
  Brian Kondracki, Babak Amin Azad *(Stony Brook University)*, Oleksii Starov *(Palo Alto Networks)*,
  Nick Nikiforakis *(Stony Brook University)*
- **Reverse Attack: Black-box Attacks on Collaborative Recommendation** 51
  Yihe Zhang, Xu Yuan *(University of Louisiana at Lafayette)*, Jin Li *(Guangzhou University)*,
  Jiadong Lou, Li Chen, Nian-Feng Tzeng *(University of Louisiana at Lafayette)*
- **It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications** 69
  Qingying Hao, Licheng Luo, Steve T.K. Jan, Gang Wang *(University of Illinois at Urbana-Champaign)*

Session 1B: Attacks and Robustness

- **Black-box Adversarial Attacks on Commercial Speech Platforms with Minimal Information** 86
  Baolin Zheng, Peipei Jiang, Qian Wang *(Wuhan University)*, Qi Li *(Tsinghua University)*,
  Chao Shen *(Xi'an Jiaotong University)*, Cong Wang *(City University of Hong Kong)*,
  Yunjie Ge, Qingyang Teng, Shenyi Zhang *(Wuhan University)*
- **A Hard Label Black-box Adversarial Attack Against Graph Neural Networks** 108
  Jiaming Mu *(Tsinghua University)*, Binghui Wang *(Illinois Institute of Technology)*,
  Qi Li *(Tsinghua University)*, Kun Sun *(George Mason University)*,
  Mingwei Xu, Zhuotao Liu *(Tsinghua University)*
- **Robust Adversarial Attacks Against DNN-Based Wireless Communication Systems** 126
  Alireza Bahramali, Milad Nasr, Amir Houmansadr, Dennis Goeckel,
  Don Towsley *(University of Massachusetts, Amherst)*
- **AI-Lancet: Locating Error-inducing Neurons to Optimize Neural Networks** 141
  Yue Zhao, Hong Zhu *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*,
  Kai Chen *(Institute of Information Engineering, Chinese Academy of Sciences & China University of Chinese Academy of Sciences, China & Beijing Academy of Artificial Intelligence)*,
  Shengzhi Zhang *(Metropolitan College, Boston University)*

Session 1C: Zero Knowledge I

- **Doubly Efficient Interactive Proofs for General Arithmetic Circuits with Linear Prover Time** 159
  Jiaheng Zhang *(University of California, Berkeley)*, Tianyi Liu *(Texas A&M University)*,
  Weijie Wang *(Shanghai Jiao Tong University)*, Yinuo Zhang, Dawn Song *(University of California, Berkeley)*,
  Xiang Xie *(Shanghai Key Laboratory of Privacy-Preserving Computation)*, Yupeng Zhang *(Texas A&M University)*
- **Constant-Overhead Zero-Knowledge for RAM Programs** 178
  Nicholas Franzese *(Northwestern University)*, Jonathan Katz *(University of Maryland)*,
  Steve Lu *(Stealth Software Technologies, Inc.)*, Rafail Ostrovsky *(University of California, Los Angeles)*,
  Xiao Wang, Chenkai Weng *(Northwestern University)*
- **Appenzeller to Brie: Efficient Zero-Knowledge Proofs for Mixed-Mode Arithmetic and $\mathbb{Z}_{2^k}$** . 192
  Carsten Baum, Lennart Braun *(Aarhus University)*, Alexander Munch-Hansen *(Aarhus University)*,
  Benoit Razet *(Galois, Inc.)*, Peter Scholl *(Aarhus University)*
- **Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices** 212
  Yuval Ishai *(Technion)*, Hang Su *(University of Virginia)*,
  David J. Wu *(University of Texas at Austin)*

Session 1D: Authentication and Click Fraud

- **"Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World** 235
  Emily Wenger, Max Bronckers, Christian Cianfarani, Jenna Cryan, Angela Sha, Haitao Zheng,
  Ben Y. Zhao *(University of Chicago)*
- **Don't Forget the Stuffing! Revisiting the Security Impact of Typo-Tolerant Password Authentication** 252
  Sena Sahin, Frank Li *(Georgia Institute of Technology)*
- **Dissecting Click Fraud Autonomy in the Wild** 271
  Tong Zhu, Yan Meng, 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** 287
  Suibin Sun, Le Yu *(Shanghai Jiao Tong University)*, Xiaokuan Zhang *(The Ohio State University)*,
  Minhui Xue *(The University of Adelaide)*, Ren Zhou, Haojin Zhu *(Shanghai Jiao Tong University)*,
  Shuang Hao *(University of Texas at Dallas)*, Xiaodong Lin *(University of Guelph)*
- **Usable User Authentication on a Smartwatch using Vibration** 304
  Sunwoo Lee *(Korea University)*, Wonsuk Choi *(Hansung University)*, Dong Hoon Lee *(Korea University)*

Session 2A: Fuzzing and Bug Finding

- **Automated Bug Hunting With Data-Driven Symbolic Root Cause Analysis** 320
  Carter Yagemann, Simon P. Chung, Brendan Saltaformaggio, Wenke Lee *(Georgia Institute of Technology)*
- **SNIPUZZ: Black-box Fuzzing of IoT Firmware via Message Snippet Inference** 337
  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, Surya Nepal *(CSIRO Data61)*,
  Yang Xiang *(Swinburne University of Technology)*
- **Same Coverage, Less Bloat: Accelerating Binary-only Fuzzing with Coverage-preserving Coverage-guided Tracing** 351
  Stefan Nagy *(Virginia Tech)*, Anh Nguyen-Tuong *(University of Virginia)*,
  Jason D. Hiser, Jack W. Davidson *(University of Virginia)*, Matthew Hicks *(Virginia Tech)*
- **HyperFuzzer: An Efficient Hybrid Fuzzer for Virtual CPUs** 366
  Xinyang Ge *(Microsoft Research)*, Ben Niu *(Microsoft)*, Robert Brotzman *(Penn State University)*,
  Yaohui Chen *(Facebook)*, HyungSeok Han *(Korea Advanced Institute of Science and Technology)*,
  Patrice Godefroid, Weidong Cui *(Microsoft Research)*
- **HARDSHEAP: A Universal and Extensible Framework for Evaluating Secure Allocators** 379
  Insu Yun, Woosun Song, Seunggi Min *(Korea Advanced Institute of Science and Technology)*,
  Taesoo Kim *(Georgia Institute of Technology)*

Session 2B: Formal Analysis and Verification

- **DPGen: Automated Program Synthesis for Differential Privacy** 393
  Yuxin Wang, Zeyu Ding, Yingtai Xiao, Daniel Kifer, Danfeng Zhang *(The Pennsylvania State University)*
- **A Formally Verified Configuration for Hardware Security Modules in the Cloud** 412
  Riccardo Focardi, Flaminia L. Luccio *(Ca' Foscari University)*
- **Solver-Aided Constant-Time Hardware Verification** 429
  Klaus v. Gleissenthall *(Vrije Universiteit Amsterdam)*,
  Rami Gökhan Kıcı, Deian Stefan, Ranjit Jhala *(University of California, San Diego)*
- **Exorcising Spectres with Secure Compilers** 445
  Marco Patrignani *(CISPA Helmholtz Center for Information Security)*,
  Marco Guarnieri *(IMDEA Software Institute)*
- **Structured Leakage and Applications to Cryptographic Constant-Time and Cost** 462
  Gilles Barthe *(MPI-SP & IMDEA Software Institute)*, Benjamin Grégoire *(Université Côte d'Azur, Inria)*,
  Vincent Laporte *(Université de Lorraine, CNRS, Inria, LORIA, F-54000)*,
  Swarn Priya *(Université Côte d'Azur, Inria)*

Session 2C: Defenses for ML Robustness

- **Learning Security Classifiers with Verified Global Robustness Properties** 477
  Yizheng Chen *(University of California, Berkeley)*, Shiqi Wang *(Columbia University)*,
  Yue Qin, Xiaojing Liao *(Indiana University Bloomington)*, Suman Jana *(Columbia University)*,
  David Wagner *(University of California, Berkeley)*
- **On the Robustness of Domain Constraints** 495
  Ryan Sheatsley, Blaine Hoak, Eric Pauley, Yohan Beugin *(The Pennsylvania State University)*,
  Michael J. Weisman *(United States Army Research Laboratory)*,
  Patrick McDaniel *(The Pennsylvania State University)*
- **CERT-RNN: Towards Certifying the Robustness of Recurrent Neural Networks** 516
  Tianyu Du *(Zhejiang University)*, Shouling Ji *(Zhejiang University & Binjiang Institute of Zhejiang University)*,
  Lujia Shen, Yao Zhang, Jinfeng Li *(Zhejiang University)*,
  Jie Shi *(Huawei International, Singapore)*, Chengfang Fang *(Huawei International, Singapore)*,
  Jianwei Yin *(Zhejiang University & Binjiang Institute of Zhejiang University)*,
  Raheem Beyah *(Georgia Institute of Technology)*, Ting Wang *(The Pennsylvania State University)*
- **TSS: Transformation-Specific Smoothing for Robustness Certification** 535
  Linyi Li *(University of Illinois)*, Maurice Weber *(ETH Zürich)*, Xiaojun Xu *(University of Illinois)*,
  Luka Rimanic *(ETH Zürich)*, Bhavya Kailkhura *(Lawrence Livermore National Laboratory)*,
  Tao Xie *(Peking University)*, Ce Zhang *(ETH Zürich)*, Bo Li *(University of Illinois)*

Session 2D: Secure Multiparty Computation

- **Efficient Online-friendly Two-Party ECDSA Signature** 558
  Haiyang Xue *(Institute of Information Engineering, Chinese Academy of Sciences & 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, Handong Cui *(The University of Hong Kong)*
- **One Hot Garbling** 574
  David Heath, Vladimir Kolesnikov *(Georgia Institute of Technology)*
- **The Return of Eratosthenes: Secure Generation of RSA Moduli using Distributed Sieving** 594
  Cyprien Delpech de Saint Guilhem *(KU Leuven)*,
  Eleftheria Makri *(KU Leuven & Saxion University of Applied Sciences)*,
  Dragos Rotaru *(KU Leuven & Cape Privacy)*, Titouan Tanguy *(KU Leuven)*
- **Secure Graph Analysis at Scale** 610
  Toshinori Araki, Jun Furukawa *(NEC Corporation)*, Kazuma Ohara *(AIST)*,
  Benny Pinkas, Hanan Rosemarin *(Bar-Ilan University)*, Hikaru Tsuchida *(NEC Corporation)*
- **Oblivious Linear Group Actions and Applications** 630
  Nuttapong Attrapadung, Goichiro Hanaoaka, Takahiro Matsuda *(AIST)*,
  Hiraku Morita *(University of St. Gallen)*, Kazuma Ohara, Jacob C. N. Schuldt, Tadanori Teruya *(AIST)*,
  Kazunari Tozawa *(University of Tokyo)*

Session 3A: Side Channel

- **Wireless Charging Power Side-Channel Attacks** 651
  Alexander S. La Cour *(Princeton University)*, Khurram K. Afridi, G. Edward Suh *(Cornell University)*

- **Indistinguishability Prevents Scheduler Side Channels in Real-Time Systems** 666
  Chien-Ying Chen, Debopam Sanyal *(University of Illinois at Urbana-Champaign)*,
  Sibin Mohan *(Oregon State University)*

- **ROSITA++: Automatic Higher-Order Leakage Elimination from Cryptographic Code** 685
  Madura A. Shelton *(University of Adelaide)*, Łukasz Chmielewski *(Radboud University and Riscure)*,
  Niels Samwel *(Radboud University)*, Markus Wagner *(University of Adelaide)*,
  Lejla Batina *(Radboud University)*, Yuval Yarom *(University of Adelaide)*

- **Periscope: A Keystroke Inference Attack Using Human Coupled Electromagnetic Emanations** 700
  Wenqiang Jin *(Hunan University)*, Srinivasan Murali, Huadi Zhu, Ming Li *(The University of Texas at Arlington)*

- **CONSTANTINE: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization** 715
  Pietro Borrello, Daniele Cono D'Elia, Leonardo Querzoni *(Sapienza University of Rome)*,
  Cristiano Giuffrida *(Vrije Universiteit Amsterdam)*,

Session 3B: Operating Systems

- **ECMO: Peripheral Transplantation to Rehost Embedded Linux Kernels** 734
  Muhui Jiang *(The Hong Kong Polytechnic University & Zhejiang University)*,
  Lin Ma, Yajin Zhou, Qiang Liu *(Zhejiang University)*, Cen Zhang *(Nanyang Technological University)*,
  Zhi Wang *(Florida State University)*, Xiapu Luo *(The Hong Kong Polytechnic University)*,
  Lei Wu, Kui Ren *(Zhejiang University)*

- **SyzGen: Automated Generation of Syscall Specification of Closed-Source macOS Drivers**.... 749
  Weiteng Chen *(University of California, Riverside)*, Yu Wang *(Didi Research America)*,
  Zheng Zhang, Zhiyun Qian *(University of California, Riverside)*,

- **Demons in the Shared Kernel: Abstract Resource Attacks Against OS-level Virtualization**.... 764
  Nanzi Yang *(Xidian University)*, Wenbo Shen *(Zhejiang University)*, Jinku Li *(Xidian University)*,
  Yutian Yang *(Zhejiang University)*, Kangjie Lu *(University of Minnesota, Twin Cities)*,
  Jietao Xiao *(Xidian University)*, Tianyu Zhou *(Zhejiang University)*, Chenggang Qin *(Ant Group)*,
  Wang Yu *(Ant Group)*, Jianfeng Ma *(Xidian University)*, Kui Ren *(Zhejiang University)*

- **SmashEx: Smashing SGX Enclaves Using Exceptions** 779
  Jinhua Cui *(National University of Defense Technology)*,
  Jason Zhijingcheng Yu *(National University of Singapore)*, Shweta Shinde *(ETH Zürich)*,
  Prateek Saxena *(National University of Singapore)*, Zhiping Cai *(National University of Defense Technology)*

- **CPscan: Detecting Bugs Caused by Code Pruning in IoT Kernels** 794
  Lirong Fu *(Zhejiang University)*, Shouling Ji *(Zhejiang University & Binjiang Institute of Zhejiang University)*,
  Kangjie Lu *(University of Minnesota)*, Peiyu Liu *(Zhejiang University)*,
  Xuhong Zhang *(Zhejiang University & Binjiang Institute of Zhejiang University)*,
  Yuxuan Duan, Zihui Zhang, Wenzhi Chen *(Zhejiang University)*,
  Yanjun Wu *(Institute of Software, Chinese Academy of Sciences)*

- **Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels** 811
  Hang Zhang, Weiteng Chen, Yu Hao, Guoren Li, Yizhuo Zhai, Xiaochen Zou,
  Zhiyun Qian *(University of California, Riverside)*

Session 3C: Inference Attacks

- **Honest-but-Curious Nets: Sensitive Attributes of Private Inputs Can Be Secretly Coded into the Classifiers' Outputs** 825
  Mohammad Malekzadeh, Anastasia Borovykh, Deniz Gunduz *(Imperial College London)*

- **Quantifying and Mitigating Privacy Risks of Contrastive Learning** 845
  Xinlei He, Yang Zhang *(CISPA Helmholtz Center for Information Security)*

- **Membership Inference Attacks Against Recommender Systems**.. 864
  Minxing Zhang *(Shandong University & CISPA Helmholtz Center for Information Security)*,
  Zhaochun Ren, Zihan Wang, Pengjie Ren, Zhunmin Chen, Pengfei Hu *(Shandong University)*,
  Yang Zhang *(CISPA Helmholtz Center for Information Security)*
- **Membership Leakage in Label-Only Exposures**... 880
  Zheng Li, Yang Zhang *(CISPA Helmholtz Center for Information Security)*
- **When Machine Unlearning Jeopardizes Privacy** 896
  Min Chen, Zhikun Zhang *(CISPA Helmholtz Center for Information Security)*,
  Tianhao Wang *(Carnegie Mellon University & University of Virginia)*,
  Michael Backes *(CISPA Helmholtz Center for Information Security)*, Mathias Humbert *(University of Lausanne)*,
  Yang Zhang *(CISPA Helmholtz Center for Information Security)*

Session 3D: DoS

- **Deterrence of Intelligent DDoS via Multi-Hop Traffic Divergence**... 923
  Yuanjie Li, Hewu Li, Zhizheng Lv, Xingkun Yao *(Tsinghua University)*,
  Qianru Li *(University of California, Los Angeles)*, Jianping Wu *(Tsinghua University)*
- **Scan, Test, Execute: Adversarial Tactics in Amplification DDoS Attacks** 940
  Harm Griffioen *(Hasso Plattner Institute)*, Kris Oosthoek *(Technische Universiteit Delft)*,
  Paul van der Knaap *(Technische Universiteit Delft)*, Christian Doerr *(Hasso Plattner Institute)*
- **Warmonger: Inflicting Denial-of-Service via Serverless Functions in the Cloud**....................... 955
  Junjie Xiong *(University of South Florida)*, Mingkui Wei *(George Mason University)*,
  Zhuo Lu, Yao Liu *(University of South Florida)*
- **United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale** 970
  Daniel Wagner *(DE-CIX & Max Planck Institute for Informatics)*, Daniel Kopp *(DE-CIX)*,
  Matthias Wichtlhuber *(DE-CIX)*, Christoph Dietzel *(DE-CIX & Max Planck Institute for Informatics)*,
  Oliver Hohlfeld *(Brandenburg University of Technology)*, Georgios Smaragdakis *(TU Delft)*,
  Anja Feldmann *(Max Planck Institute for Informatics)*

Session 4A: Modeling Blockchains and Distributed Ledgers

- **Revisiting Nakamoto Consensus in Asynchronous Networks: A Comprehensive Analysis of Bitcoin Safety and ChainQuality** 988
  Muhammad Saad, Afsah Anwar *(University of Central Florida)*,
  Srivatsan Ravi *(University of Southern California)*, David Mohaisen *(University of Central Florida)*
- **How Does Blockchain Security Dictate Blockchain Implementation?**...................................... 1006
  Andrew Lewis-Pye *(London School of Economics)*, Tim Roughgarden *(Columbia University)*
- **The Exact Security of BIP32 Wallets** 1020
  Poulami Das, Andreas Erwig, Sebastian Faust *(Technische Universität Darmstadt)*,
  Julian Loss *(University of Maryland)*, Siavash Riahi *(Technische Universität Darmstadt)*
- **A Security Framework for Distributed Ledgers** 1043
  Mike Graf, Daniel Rausch *(University of Stuttgart)*,
  Viktoria Ronge, Christoph Egger *(Friedrich-Alexander University Erlangen-Nürnberg)*,
  Ralf Küsters *(University of Stuttgart)*,
  Dominique Schröder *(Friedrich-Alexander University Erlangen-Nürnberg)*

Session 4B: Wireless, Mobile, and IoT

- **This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration** 1065
  Michalis Diamantaris, Serafeim Moustakas *(FORTH)*, Lichao Sun *(Lehigh University)*,
  Sotiris Ioannidis *(Technical University of Crete)*, Jason Polakis *(University of Illinois at Chicago)*
- ***Noncompliance as Deviant Behavior:* An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices** 1082
  Syed Rafiul Hussain *(The Pennsylvania State University)*, Imtiaz Karim *(Purdue University)*,
  Abdullah Al Ishtiaq *(The Pennsylvania State University)*, Omar Chowdhury *(University of Iowa)*,
  Elisa Bertino *(Purdue University)*

- **All your Credentials are Belong to Us: On Insecure WPA2-Enterprise Configurations** 1100
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-device IoT Certificate Revocation Checking with Small Memory and Low Latency** 1118
Xiaofeng Shi, Shouqian Shi, Minmei Wang, Jonne Kaunisto, Chen Qian *(University of California, Santa Cruz)*

Session 4C: Private Set Intersection

- **Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication** 1135
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)*

- **Simple, Fast Malicious Multiparty Private Set Intersection** 1151
Ofri Nevo *(Open University of Israel)*, Ni Trieu *(Arizona State University)*, Avishay Yanai *(VMware Research)*

- **Compact and Malicious Private Set Intersection for Small Sets** 1166
Mike Rosulek *(Oregon State University)*, Ni Trieu *(Arizona State University)*

- **Efficient Linear Multiparty PSI and Extensions to Circuit/Quorum PSI** 1182
Nishanth Chandran *(Microsoft Research)*, Nishka Dasgupta *(Aarhus University)*, Divya Gupta, Sai Lakshmi Bhavana Obbattu *(Microsoft Research)*, Sruthi Sekar *(Indian Institute of Science)*, Akash Shah *(University of California, Los Angeles)*

Session 4D: Differential Privacy

- **Differential Privacy for Directional Data** 1205
Benjamin Weggenmann *(SAP Security Research)*, Florian Kerschbaum *(University of Waterloo)*

- **Differentially Private Sparse Vectors with Low Error, Optimal Space, and Fast Access** 1223
Martin Aumüller *(IT University of Copenhagen)*, Christian Janos Lebeda, Rasmus Pagh *(Basic Algorithms Research Copenhagen & University of Copenhagen)*

- **Continuous Release of Data Streams under both Centralized and Local Differential Privacy** 1237
Tianhao Wang *(Carnegie Mellon University & University of Virginia)*, Joann Qiongna Chen *(University of California, Irvine)*, Zhikun Zhang *(CISPA Helmholtz Center for Information Security)*, Dong Su *(Alibaba Inc.)*, Yueqiang Cheng *(NIO Security Research)*, Zhou Li *(University of California, Irvine)*, Ninghui Li *(Purdue University)*, Somesh Jha *(University of Wisconsin, Madison)*

- **Side-Channel Attacks on Query-Based Data Anonymization** 1254
Franziska Boenisch *(Fraunhofer AISEC)*, Reinhard Munz *(Max Planck Institute for Software Systems)*, Marcel Tiepelt *(Karlsruhe Institute of Technology)*, Simon Hanisch *(TU Dresden)*, Christiane Kuhn *(Karlsruhe Institute of Technology)*, Paul Francis *(Max Planck Institute for Software Systems)*

- **AHEAD: Adaptive Hierarchical Decomposition for Range Query under Local Differential Privacy** 1266
Linkang Du *(Zhejiang University)*, Zhikun Zhang *(CISPA Helmholtz Center for Information Security)*, Shaojie Bai *(Zhejiang University)*, Changchang Liu *(IBM Research)*, Shouling Ji *(Zhejiang University & Binjiang Institute of Zhejiang University)*, Peng Cheng *(Zhejiang University)*, Jiming Chen *(Zhejiang University & Zhejiang University of Technology)*

Session 5A: Control System Security

- **Who's In Control? On Security Risks of Disjointed IoT Device Management Channels** 1289
  Yan Jia *(Nankai University & Xidian University & Indiana University Bloomington)*,
  Bin Yuan *(Huazhong University of Science and Technology & Indiana University Bloomington)*,
  Luyi Xing, Dongfang Zhao, Yifan Zhang, XiaoFeng Wang *(Indiana University Bloomington)*,
  Yijing Liu *(Nankai University)*, Kaimin Zheng *(Huazhong University of Science and Technology)*,
  Peyton Crnjak *(Indiana University Bloomington)*,
  Yuqing Zhang *(University of Chinese Academy of Sciences & Xidian University & Hainan University)*,
  Deqing Zou, Hai Jin *(Huazhong University of Science and Technology)*

- **DroneKey: A Drone-Aided Group-Key Generation Scheme for Large-Scale IoT Networks**.. 1306
  Dianqi Han, Ang Li, Jiawei Li, Yan Zhang *(Arizona State University)*,
  Tao Li *(Indiana University–Purdue University Indianapolis)*, Yanchao Zhang *(Arizona State University)*

- **You Make Me Tremble: A First Look at Attacks Against Structural Control Systems**............ 1320
  Abel Zambrano *(Universidad de Los Andes)*, Alejandro Palacio Betancur *(The Pennsylvania 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 *(The Pennsylvania State University)*, Jairo Giraldo *(University of Utah)*,
  Alvaro A. Cardenas *(University of California, Santa Cruz)*

- **MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets** 1338
  Tohid Shekari, Celine Irvene *(Georgia Institute of Technology)*,
  Alvaro A. Cardenas *(University of California, Santa Cruz)*, Raheem Beyah *(Georgia Institute of Technology)*

- **AION: Enabling Open Systems through Strong Availability Guarantees for Enclaves** 1357
  Fritz Alder, Jo Van Bulck, Frank Piessens, Jan Tobias Mühlberg *(KU Leuven)*

Session 5B: PKI and Access Control

- **Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem**.. 1373
  Yiming Zhang *(Tsinghua University & Beijing National Research Center for Information Science and Technology)*,
  Baojun Liu *(Tsinghua University)*, Chaoyi Lu *(Tsinghua University & 360Netlab)*,
  Zhou Li *(University of California, Irvine)*,
  Haixin Duan *(Tsinghua University & QI-ANXIN Technology Research Institute)*,
  Jiachen Li *(Tsinghua University)*, Zaifeng Zhang *(360Netlab)*

- **On Re-engineering the X.509 PKI with Executable Specification for Better Implementation Guarantees** 1388
  Joyanta Debnath *(The University of Iowa)*, Sze Yiu Chau *(The Chinese University of Hong Kong)*,
  Omar Chowdhury *(The University of Iowa)*

- **APECS: A Distributed Access Control Framework for Pervasive Edge Computing Services** 1405
  Sean Dougherty, Reza Tourani *(Saint Louis University)*,
  Gaurav Panwar, Roopa Vishwanathan, Satyajayant Misra *(New Mexico State University)*,
  Srikathyayani Srikanteswara *(Intel Corp.)*

- **Let's Downgrade Let's Encrypt** 1421
  Tianxiang Dai, Haya Shulman *(ATHENE Center & Fraunhofer SIT)*,
  Michael Waidner *(ATHENE Center; TU Darmstadt; & Fraunhofer SIT)*

Session 5C: Messaging and Privacy

- **A Concrete Treatment of Efficient Continuous Group Key Agreement via Multi-Recipient PKEs** 1441
  Keitaro Hashimoto *(Tokyo Institute of Technology & AIST)*, Shuichi Katsumata *(AIST)*,
  Eamonn Postlethwaite *(CWI)*, Thomas Prest *(PQShield SAS)*, Bas Westerbaan *(Cloudflare)*

- **Modular Design of Secure Group Messaging Protocols and the Security of MLS** 1463
  Joël Alwen *(AWS Wickr)*, Sandro Coretti *(IOHK)*, Yevgeniy Dodis *(New York University)*,
  Yiannis Tselekounis *(University of Edinburgh)*

- **Secure Complaint-Enabled Source-Tracking for Encrypted Messaging** 1484
Charlotte Peale *(Stanford University)*, Saba Eskandarian *(UNC Chapel Hill)*,
Dan Boneh *(Stanford University)*
- **Fuzzy Message Detection** 1507
Gabrielle Beck *(Johns Hopkins University)*, Julia Len *(Cornell University)*,
Ian Miers *(University of Maryland)*, Matthew Green *(Johns Hopkins University)*
- **Meteor: Cryptographically Secure Steganography for Realistic Distributions** 1529
Gabriel Kaptchuk *(Boston University)*,
Tushar M. Jois, Matthew Green, Aviel D. Rubin *(Johns Hopkins University)*
- **Hiding the Lengths of Encrypted Messages via Gaussian Padding** 1549
Jean Paul Degabriele *(Technische Universität Darmstadt)*

Session 5D: Misc: Android and Vulnerabilities

- **Android on PC: On the Security of End-user Android Emulators** 1566
Fenghao Xu, 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)*
- **Ghost in the Binder: Binder Transaction Redirection Attacks in Android System Services** .. 1581
Xiaobo Xiang *(Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences; Alpha Lab; and 360 Government & Enterprise Security Group)*,
Ren Zhang *(Nervos & Shandong Institute of Blockchain)*, Hanxiang Wen *(Ant Group)*,
Xiaorui Gong, Baoxu Liu *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*
- **Dissecting Residual APIs in Custom Android ROMs** 1598
Zeinab El-Rewini, Yousra Aafer *(University of Waterloo)*
- **VIP: Safeguard Value Invariant Property for Thwarting Critical Memory Corruption Attacks** 1612
Mohannad Ismail, Jinwoo Yom, Christopher Jelesnianski *(Virginia Polytechnic Institute and State University)*,
Yeongjin Jang *(Oregon State University)*, Changwoo Min *(Virginia Polytechnic Institute and State University)*
- **Detecting Missed Security Operations Through Differential Checking of Object-based Similar Paths** 1627
Dinghao Liu *(Zhejiang University)*, Qiushi Wu *(University of Minnesota)*,
Shouling Ji *(Zhejiang University & Binjiang Institution of Zhejiang University)*,
Kangjie Lu *(University of Minnesota)*, Zhenguang Liu *(Zhejiang University)*,
Jianhai Chen, Qinming He *(Zhejiang University)*

Session 6A: Consensus and Attacks

- **DETER: Denial of Ethereum Txpool sERvices** 1645
Kai Li, Yibo Wang, Yuzhe Tang *(Syracuse University)*
- **SyncAttack: Double-spending in Bitcoin Without Mining Power** 1668
Muhammad Saad, Songqing Chen, David Mohaisen *(University of Central Florida)*
- **Multi-Threshold Byzantine Fault Tolerance** 1686
Atsuki Momose *(Intelligent Systems Laboratory, SECOM CO., LTD. & Nagoya University)*,
Ling Ren *(University of Illinois at Urbana-Champaign)*
- **Securing Parallel-chain Protocols under Variable Mining Power** 1700
Xuechao Wang *(University of Illinois at Urbana-Champaign)*,
Viswa Virinchi Muppirala *(University of Washington at Seattle)*,
Lei Yang *(Massachusetts Institute of Technology)*, Sreeram Kannan *(University of Washington at Seattle)*,
Pramod Viswanath *(University of Illinois at Urbana-Champaign)*
- **BFT Protocol Forensics** 1722
Peiyao Sheng, Gerui Wang *(University of Illinois at Urbana-Champaign)*, Kartik Nayak *(Duke University)*,
Sreeram Kannan *(University of Washington)*, Pramod Viswanath *(University of Illinois at Urbana-Champaign)*

Session 6B: Web Vulnerabilities

- **Supply-Chain Vulnerability Elimination via Active Learning and Regeneration** 1755
  Nikos Vasilakis *(Massachusetts Institute of Technology)*,
  Achilles Benetopoulos *(University of California, Santa Cruz)*,
  Shivam Handa, Alizee Schoen, Jiasi Shen, Martin C. Rinard *(Massachusetts Institute of Technology)*
- **XSinator.com: From a Formal Model to the Automatic Evaluation of Cross-Site Leaks in Web Browsers** 1771
  Lukas Knittel, Christian Mainka *(Ruhr University Bochum)*,
  Marcus Niemietz *(Niederrhein University of Applied Sciences)*,
  Dominik Trevor Noß *(Ruhr University Bochum)*, Jörg Schwenk *(Ruhr University Bochum)*
- **DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale** 1789
  Aurore Fass, Dolière Francis Somé, Michael Backes,
  Ben Stock *(CISPA Helmholtz Center for Information Security)*,
- **T-Reqs: HTTP Request Smuggling with Differential Fuzzing** 1805
  Bahruz Jabiyev, Steven Sprecher *(Northeastern University)*, Kaan Onarlioglu *(Akamai Technologies)*,
  Engin Kirda *(Northeastern University)*
- **Preventing Dynamic Library Compromise on Node.js via RWX-Based Privilege Reduction** 1821
  Nikos Vasilakis *(Massachusetts Institute of Technology)*,
  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)*,
- **Spinner: Automated Dynamic Command Subsystem Perturbation** 1839
  Meng Wang, Chijung Jung, Ali Ahad, Yonghwi Kwon *(University of Virginia)*

Session 6C: Audio Systems and Autonomous Driving

- ***FakeWake:* Understanding and Mitigating Fake Wake-up Words of Voice Assistants** 1861
  Yanjiao Chen, Yijie Bai *(Zhejiang University)*, Richard Mitev *(Technical University of Darmstadt)*,
  Kaibo Wang *(Zhejiang University)*, Ahmad-Reza Sadeghi *(Technical University of Darmstadt)*,
  Wenyuan Xu *(Zhejiang University)*
- **Robust Detection of Machine-induced Audio Attacks in Intelligent Audio Systems with Microphone Array** 1884
  Zhuohang Li *(University of Tennessee)*, Cong Shi, Tianfang Zhang, Yi Xie *(Rutgers University)*,
  Jian Liu *(University of Tennessee)*, Bo Yuan, Yingying Chen *(Rutgers University)*
- **Glowworm Attack: Optical TEMPEST Sound Recovery via a Device's Power Indicator LED** 1900
  Ben Nassi, Yaron Pirutin, Tomer Galor, Yuval Elovici, Boris Zadov *(Ben-Gurion University of the Negev)*
- **CapSpeaker: Injecting Voices to Microphones via Capacitors** 1915
  Xiaoyu Ji, Juchuan Zhang, Shui Jiang, Jishen Li, Wenyuan Xu *(Zhejiang University)*
- **I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights** 1930
  Wei Wang, Yao Yao, Xin Liu *(University of Maryland, Baltimore County)*,
  Xiang Li *(Cambricon SingGo)*, Pei Hao, Ting Zhu *(University of Maryland, Baltimore County)*
- **Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?** 1945
  Yi Zhu *(State University of New York at Buffalo)*, Chenglin Miao *(University of Georgia)*,
  Tianhang Zheng *(University of Toronto)*, Foad Hajiaghajani *(State University of New York at Buffalo)*,
  Lu Su *(Purdue University)*, Chunming Qiao *(State University of New York at Buffalo)*

Session 6D: Authentication and Privacy

- **A PKI-based Framework for Establishing Efficient MPC Channels** 1961
  Daniel Masny, Gaven Watson *(VISA Research)*
- **The Security of ChaCha20-Poly1305 in the Multi-User Setting** 1981
  Jean Paul Degabriele, Jérôme Govinden *(Technische Universität Darmstadt)*,
  Felix Günther, Kenneth G. Paterson *(ETH Zurich)*

- **With a Little Help from My Friends: Constructing Practical Anonymous Credentials** 2004
  Lucjan Hanzlik *(CISPA Helmholtz Center for Information Security)*,
  Daniel Slamanig *(AIT Austrian Institute of Technology)*
- **Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees** 2024
  Matthew Weidner *(Carnegie Mellon University)*,Martin Kleppmann, Daniel Hugenroth *(University of Cambridge)*,
  Alastair R. Beresford *(University of Cambridge)*
- **Revisiting Fuzzy Signatures: Towards a More Risk-Free Cryptographic Authentication System based on Biometrics** 2046
  Shuichi Katsumata, Takahiro Matsuda *(AIST)*, Wataru Nakamura *(Hitachi, Ltd.)*,
  Kazuma Ohara *(AIST)*, Kenta Takahashi *(Hitachi, Ltd.)*
- **On the (In)Security of ElGamal in OpenPGP** 2066
  Luca De Feo, Bertram Poettering, Alessandro Sorniotti *(IBM Research Europe - Zurich)*

Session 7A: Privacy Attacks and Defenses for ML

- **EncoderMI: Membership Inference against Pre-trained Encoders in Contrastive Learning** 2081
  Hongbin Liu, Jinyuan Jia *(Duke University)*,
  Wenjie Qu *(Huazhong University of Science and Technology)*, Neil Zhenqiang Gong *(Duke University)*
- **TableGAN-MCA: Evaluating Membership Collisions of GAN-Synthesized Tabular Data Releasing** 2096
  Aoting Hu, Renjie Xie *(Southeast University)*, Zhigang Lu *(Macquarie University)*,
  Aiqun Hu *(Southeast University)*, Minhui Xue *(The University of Adelaide)*
- **Unleashing the Tiger: Inference Attacks on Split Learning** 2113
  Dario Pasquini *(Sapienza University of Rome & Institute of Applied Computing, IAC-CNR)*,
  Giuseppe Ateniese *(George Mason University)*, Massimo Bernaschi *(Institute of Applied Computing, IAC-CNR)*
- **Locally Private Graph Neural Networks** 2130
  Sina Sajadmanesh, Daniel Gatica-Perez *(Idiap Research Institute & EPFL)*
- **DataLens: Scalable Privacy Preserving Training via Gradient Compression and Aggregation** 2146
  Boxin Wang, Fan Wu, Yunhui Long *(University of Illinois at Urbana-Champaign)*,
  Luka Rimanic, Ce Zhang *(ETH Zürich)*, Bo Li *(University of Illinois at Urbana-Champaign)*

Session 7B: Fuzzing

- **Regression Greybox Fuzzing** 2169
  Xiaogang Zhu *(Swinburne University of Technology)*, Marcel Böhme *(Monash University)*
- **MirChecker: Detecting Bugs in Rust Programs via Static Analysis** 2183
  Zhuohua Li, Jincheng Wang *(The Chinese University of Hong Kong)*, Mingshen Sun *(Baidu Security)*,
  John C.S. Lui *(The Chinese University of Hong Kong)*
- **V-SHUTTLE: Scalable and Semantics-Aware Hypervisor Virtual Device Fuzzing** 2197
  Gaoning Pan *(Zhejiang University & Ant Group)*, Xingwei Lin *(Ant Group)*,
  Xuhong Zhang *(Zhejiang University & Binjiang Institute of Zhejiang University)*,
  Yongkang Jia *(Zhejiang University)*, Shouling Ji *(Zhejiang University & Binjiang Institute of Zhejiang University)*,
  Chunming Wu *(Zhejiang University)*, Xinlei Ying, Jiashui Wang *(Ant Group)*,
  Yanjun Wu *(Institute of Software, Chinese Academy of Sciences)*
- **Hardware Support to Improve Fuzzing Performance and Precision** 2214
  Ren Ding, Yonghae Kim, Fan Sang, Wen Xu, Gururaj Saileshwar, Taesoo Kim *(Georgia Institute of Technology)*
- **SoFi: Reflection-Augmented Fuzzing for JavaScript Engines** 2229
  Xiaoyu He *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*, Xiaofei Xie *(Nanyang Technological University)*,
  Yuekang Li *(Nanyang Technological University)*, Jianwen Sun *(Huawei Technologies)*,
  Feng Li, Wei Zou *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*, Yang Liu *(Nanyang Technological University)*,
  Lei Yu, Jianhua Zhou *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*, Wenchang Shi *(Renmin University of China)*, Wei Huo *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*

Session 7C: Database and Privacy

- **Reconstructing with Less: Leakage Abuse Attacks in Two Dimensions** 2243
  Evangelia Anna Markatou *(Brown University)*, Francesca Falzon *(University of Chicago)*,
  Roberto Tamassia, William Schor *(Brown University)*
- **Ɛpsolute: Efficiently Querying Databases While Providing Differential Privacy** 2262
  Dmytro Bogatov *(Boston University)*, Georgios Kellaris *(Independent Researcher)*,
  George Kollios *(Boston University)*, Kobbi Nissim *(Georgetown University)*,
  Adam O'Neill *(University of Massachusetts, Amherst)*
- **Compressed Oblivious Encoding for Homomorphically Encrypted Search** 2277
  Seung Geol Choi *(United States Naval Academy)*, Dana Dachman-Soled *(University of Maryland)*,
  S. Dov Gordon *(George Mason University)*, Linsheng Liu *(George Washington University)*,
  Arkady Yerukhimovich *(George Washington University)*
- **OnionPIR: Response Efficient Single-Server PIR** 2292
  Muhammad Haris Mughees *(University of Illinois at Urbana-Champaign)*,
  Hao Chen *(Facebook)*, Ling Ren *(University of Illinois at Urbana-Champaign)*

Session 7D: Privacy for Distributed Data and Federated Learning

- **LEAP: Leakage-Abuse Attack on Efficiently Deployable, Efficiently Searchable Encryption with Partially Known Dataset** 2307
  Jianting Ning *(Fujian Normal University & Singapore Management University)*,
  Xinyi Huang *(Fujian Normal University)*, Geong Sen Poh *(Nanyang Technological University)*,
  Jiaming Yuan, Yingjiu Li *(University of Oregon)*, Jian Weng *(Jinan University)*,
  Robert H. Deng *(Singapore Management University)*
- **On the Rényi Differential Privacy of the Shuffle Model** 2321
  Antonious M. Girgis, Deepesh Data, Suhas Diggavi *(University of California, Los Angeles)*,
  Ananda Theertha Suresh, Peter Kairouz *(Google Research)*
- **Private Hierarchical Clustering in Federated Networks** 2342
  Aashish Kolluri, Teodora Baluta, Prateek Saxena *(National University of Singapore)*
- **Secure Multi-party Computation of Differentially Private Heavy Hitters** 2361
  Jonas Böhler *(SAP Security Research)*, Florian Kerschbaum *(University of Waterloo)*

Session 8: Poster & Demo Session

- **Automated Privacy Policy Annotation with Information Highlighting Made Practical Using Deep Representations** 2378
  Abdulrahman Alabduljabbar, Ahmed Abusnaina, Ülkü Meteriz-Yildiran *(University of Central Florida)*,
  David Mohaisen *(University of Central Florida)*
- **Recovering Songs from a Hanging Light Bulb** 2381
  Ben Nassi, Yaron Pirutin, Raz Swissa *(Ben-Gurion University of the Negev)*,
  Adi Shamir *(Weizmann Institute of Science)*,
  Yuval Elovici, Boris Zadov *(Ben-Gurion University of the Negev)*
- **Search-Based Local Black-Box Deobfuscation: Understand, Improve and Mitigate (Poster)** 2384
  Grégoire Menguy, Sébastien Bardin *(Université Paris-Saclay, CEA, List)*,
  Richard Bonichon *(Nomadic Labs)*, Cauim de Souza Lima *(Université Paris-Saclay, CEA, List)*
- **Membership Inference Attacks against GANs by Leveraging Over-representation Regions** 2387
  Hailong Hu, Jun Pang *(University of Luxembourg)*
- **Earable Authentication via Acoustic Toothprint** 2390
  Zi Wang, Yili Ren *(Florida State University)*, Yingying Chen *(Rutgers University)*,
  Jie Yang *(Florida State University)*
- **POSTER: An Open-Source Framework for Developing Heterogeneous Distributed Enclave Applications** 2393
  Gianluca Scopelliti, Sepideh Pouyanrad, Job Noorman, Fritz Alder, Frank Piessens,
  Jan Tobias Mühlberg *(KU Leuven)*

- **Towards Automated Computational Auditing of mHealth Security and Privacy Regulations** 2396
  Brian Tung *(Harvard Law School)*, Zhiyuan Yu, Ning Zhang *(Washington University in St. Louis)*
- **DEMO: A Secure Voting System for Score Based Elections** 2399
  Lihi Dery *(Ariel Cyber Innovation Center & Ariel University)*,
  Tamir Tassa *(The Open University)*, Avishay Yanai *(VMware Research)*, Arthur Zamarin *(The Open University)*
- **POSTER: A Tough Nut to Crack: Attempting to Break Modulation Obfuscation** 2402
  Naureen Hoque, Hanif Rahbari *(Rochester Institute of Technology)*
- **POSTER: ReAvatar: Virtual Reality De-anonymization Attack Through Correlating Movement Signatures** 2405
  Brandon Falk, Yan Meng, Yuxia Zhan, Haojin Zhu *(Shanghai Jiao Tong University)*
- **Revisiting Hybrid Private Information Retrieval** 2408
  Daniel Günther, Thomas Schneider, Felix Wiegand *(Technical University of Darmstadt)*
- **POSTER: How Dangerous is My Click? Boosting Website Fingerprinting By Considering Sequences of Webpages** 2411
  Asya Mitseva *(Brandenburg Technical University)*,
  Jan Pennekamp, Johannes Lohmöller *(RWTH Aachen University)*,
  Torsten Ziemann, Carl Hoerchner *(Brandenburg Technical University)*,
  Klaus Wehrle *(RWTH Aachen University)*, Andriy Panchenko *(Brandenburg Technical University)*
- **Human and Organizational Factors in Public Key Certificate Authority Failures** 2414
  Skyler Johnson, Katherine Ferro, L. Jean Camp, Hilda Hadan *(Indiana University Bloomington)*
- **On Adoptability and Use Case Exploration of Threat Modeling for Mobile Communication Systems** 2417
  Hsin Yi Chen *(Aalto University)*, Siddharth Prakash Rao *(Nokia Bell Labs)*
- **Enabling Visual Analytics via Alert-driven Attack Graphs** 2420
  Azqa Nadeem, Sicco Verwer *(Delft University of Technology)*,
  Stephen Moskal, Shanchieh Jay Yang *(Rochester Institute of Technology)*
- **Predictive Cipher-Suite Negotiation for Boosting Deployment of New Ciphers** 2423
  Elias Heftrig *(ATHENE & Fraunhofer SIT)*, Jean-Pierre Seifert *(Technische Universität Berlin & Fraunhofer SIT)*,
  Haya Shulman *(ATHENE & Fraunhofer SIT)*,
  Michael Waidner *(ATHENE & TU Darmstadt & Fraunhofer SIT)*, Nils Wisiol *(Technische Universität Berlin)*
- **Chronos: Timing Interference as a New Attack Vector on Autonomous Cyber-physical Systems** 2426
  Ao Li, Jinwen Wang, Ning Zhang *(Washington University in St. Louis)*
- **Demo: Detecting Third-Party Library Problems with Combined Program Analysis** 2429
  Grigoris Ntousakis, Sotiris Ioannidis *(TU Crete)*, Nikos Vasilakis *(Massachusetts Institute of Technology)*
- **CyberBunker 2.0 - A Domain and Traffic Perspective on a Bulletproof Hoster** 2432
  Daniel Kopp *(DE-CIX)*, Eric Strehle *(Brandenburg University of Technology)*,
  Oliver Hohlfeld *(Brandenburg University of Technology)*
- **An Ontology-driven Knowledge Graph for Android Malware** 2435
  Ryan Christian, Sharmishtha Dutta *(Rensselaer Polytechnic Institute)*,
  Youngja Park *(IBM TJ Watson Research Center)*,
  Nidhi Rastogi *(Rochester Institute of Technology & Rensselaer Polytechnic Institute)*
- **De-identification of Unstructured Clinical Texts from Sequence to Sequence Perspective** .. 2438
  Md. Monowar Anjum, Noman Mohammed *(University of Manitoba)*, Xiaoqian Jiang *(University of Texas)*
- **MANIAC: A Man-Machine Collaborative System for Classifying Malware Author Groups** 2441
  Eujeanne Kim, Sung-Jun Park *(Hanyang University)*,
  Seokwoo Choi *(The Attached Institute of ETRI)*, Dong-Kyu Chae, Sang-Wook Kim *(Hanyang University)*

- **Evaluating Resilience of Domains in PKI** 2444
  Markus Brandt, Haya Shulman *(Fraunhofer SIT)*, Michael Waidner *(TU Darmstadt & Fraunhofer SIT)*
- **Demo: Large Scale Analysis on Vulnerability Remediation in Open-source JavaScript Projects** 2447
  Vinuri Bandara, Thisura Rathnayake, Nipuna Weerasekara, Charitha Elvitigala *(SCoRe Lab)*,
  Kenneth Thilakarathna *(University of Colombo)*,
  Primal Wijesekera *(University of California, Berkeley & ICSI)*,
  Kasun De Zoysa, Chamath Keppitiyagama *(University of Colombo)*
- **Optimized Predictive Control for AGC Cyber Resiliency** 2450
  Muhammad Nouman Nafees, Neetesh Saxena, Pete Burnap *(Cardiff University)*
- **POSTER: OS Independent Fuzz Testing of I/O Boundary** 2453
  Masanori Misono, Takahiro Shinagawa *(The University of Tokyo)*

Session 10A: Crypto, Symbols and Obfuscation

- **Util::Lookup: Exploiting Key Decoding in Cryptographic Libraries** 2456
  Florian Sieck, Sebastian Berndt, Jan Wichelmann, Thomas Eisenbarth *(University of Lübeck)*
- **Morpheus: Bringing The (PKCS) One To Meet the Oracle** 2474
  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, Chun Ngai Li *(The Chinese University of Hong Kong)*,
  Endadul Hoque *(Syracuse University)*, Omar Chowdhury *(The University of Iowa)*
- **PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild** 2497
  Daniel De Almeida Braga, Pierre-Alain Fouque, Mohamed Sabt *(Univ Rennes, CNRS, IRISA)*
- **Search-Based Local Black-Box Deobfuscation: Understand, Improve and Mitigate** 2513
  Grégoire Mengu, Sébastien Bardin *(Université Paris-Saclay, CEA, List)*,
  Richard Bonichon *(Nomadic Labs)*, Cauim de Souza Lima *(Université Paris-Saclay, CEA, List)*
- **Learning to Explore Paths for Symbolic Execution** 2526
  Jingxuan He, Gishor Sivanrupan, Petar Tsankov, Martin Vechev *(ETH Zürich)*

Session 10B: Crypto and Protocol Security

- **Mechanized Proofs of Adversarial Complexity and Application to Universal Composability** 2541
  Manuel Barbosa *(University of Porto (FCUP) & INESC TEC)*,
  Gilles Barthe *(MPI-SP & IMDEA Software Institute)*,
  Benjamin Grégoire *(Inria - Université Côte d'Azur)*, Adrien Koutsos *(Inria)*,
  Pierre-Yves Strub *(Institut Polytechnique de Paris)*
- **EasyPQC: Verifying Post-Quantum Cryptography** 2564
  Manuel Barbosa *(University of Porto (FCUP) and INESC TEC)*, Gilles Barthe *(MPI-SP & IMDEA Software Institute)*,
  Xiong Fan *(Algorand, Inc.)*, Benjamin Grégoire *(INRIA)*, Shih-Han Hung *(University of Texas)*,
  Jonathan Katz *(University of Maryland)*, Pierre-Yves Strub *(École Polytechnique)*,
  Xiaodi Wu *(University of Maryland)*, Li Zhou *(MPI-SP)*
- **Machine-checked ZKP for NP relations: Formally Verified Security Proofs and Implementations of MPC-in-the-Head** 2587
  José Bacelar Almeida, Manuel Barbosa, Manuel L. Correia *(University of Porto (FCUP) & INESC TEC)*,
  Karim Eldefrawy, Stéphane Graham-Lengrand *(SRI International)*,
  Hugo Pacheco *(University of Porto (FCUP) & INESC TEC)*, Vitor Pereira *(SRI International)*
- **An In-Depth Symbolic Security Analysis of the ACME Standard** 2601
  Karthikeyan Bhargavan *(INRIA Paris)*, Abhishek Bichhawat *(IIT Gandhinagar)*,
  Quoc Huy Do *(University of Stuttgart & GLIWA GmbH)*, Pedram Hosseyni *(University of Stuttgart)*,
  Ralf Küsters *(University of Stuttgart)*,
  Guido Schmitz *(University of Stuttgart and Royal Holloway University of London)*,
  Tim Würtele *(University of Stuttgart)*

- **Biometrics-Authenticated Key Exchange for Secure Messaging** 2618
Mei Wang, Kun He, Jing Chen *(Wuhan University)*, Zengpeng Li *(Shandong University)*,
Wei Zhao *(Science and Technology on Communication Security Laboratory)*,
Ruiying Du *(Wuhan University)*

- **Verifying Table-Based Elections** 2632
David Basin *(ETH Zurich)*, Jannik Dreier *(Universite de Lorraine, CNRS, Inria, LORIA)*,
Sofia Giampietro *(ETH Zürich)*, Saša Radomirović *(Heriot-Watt University)*

Session 10C: Foundations

- **Efficient CCA Timed Commitments in Class Groups** 2663
Sri Aravinda Krishnan Thyagarajan *(Friedrich Alexander Universität Erlangen-Nürnberg)*,
Guilhem Castagnos *(Université de Bordeaux, INRIA, CNRS)*,
Fabian Laguillaumie *(LIRMM, Université of Montpellier, CNRS)*,
Giulio Malavolta *(Max Planck Institute for Security and Privacy)*

- **MPC-Friendly Commitments for Publicly Verifiable Covert Security** 2685
Nitin Agrawal *(University of Oxford)*, James Bell *(The Alan Turing Institute)*,
Adrià Gascón *(Google)*, Matt J. Kusner *(University College London)*

- **Asynchronous Data Dissemination and its Applications** 2705
Sourav Das, Zhuolun Xiang, Ling Ren *(University of Illinois at Urbana-Champaign)*

- **Faster Lattice-Based KEMs via a Generic Fujisaki-Okamoto Transform Using Prefix Hashing** 2722
Julien Duman *(Ruhr-Universität Bochum)*, Kathrin Hövelmanns *(Eindhoven University of Technology)*,
Eike Kiltz *(Ruhr-Universität Bochum)*, Vadim Lyubashevsky *(IBM Research Europe)*,
Gregor Seiler *(IBM Research Europe & ETH Zurich)*

- **PPE Circuits for Rational Polynomials** 2738
Susan Hohenberger *(Johns Hopkins University)*,
Satyanarayana Vusirikala *(University of Texas at Austin)*

- **Amortized Threshold Symmetric-key Encryption** 2758
Mihai Christodorescu *(Visa Research)*, Sivanarayana Gaddam *(C3 Inc.)*,
Pratyay Mukherjee *(Visa Research)*, Rohit Sinha *(Swirlds Inc.)*

Session 10D: Applied Privacy

- **The Invisible Shadow: How Security Cameras Leak Private Activities** 2780
Jian Gong *(Central South University)*, Xinyu Zhang *(University of California San Diego)*,
Ju Ren *(Tsinghua University)*, Yaoxue Zhang *(Tsinghua University)*

- **The One-Page Setting: A Higher Standard for Evaluating Website Fingerprinting Defenses** 2794
Tao Wang *(Simon Fraser University)*

- **WristPrint: Characterizing User Re-identification Risks from Wrist-worn Accelerometry Data** 2807
Nazir Saleheen, Md Azim Ullah *(University of Memphis)*,
Supriyo Chakraborty *(IBM T. J. Watson Research Center)*,
Deniz S. Ones *(University of Minnesota)*, Mani Srivastava *(University of California, Los Angeles)*,
Santosh Kumar *(University of Memphis)*

- **Consistency Analysis of Data-Usage Purposes in Mobile Apps** 2824
Duc Bui, Yuan Yao, Kang G. Shin *(University of Michigan)*, Jong-Min Choi *(Samsung Research)*,
Junbum Shin *(CryptoLab)*

- **SugarCoat: Programmatically Generating Privacy-Preserving, Web-Compatible Resource Replacements for Content Blocking** 2844
Michael Smith *(University of California, San Diego)*, Pete Snyder *(Brave Software)*,
Benjamin Livshits *(Brave Software)*, Deian Stefan *(University of California, San Diego)*

Session 11A: Attestation and Firmware Security

- **Towards Transparent and Stealthy Android OS Sandboxing via Customizable Container-Based Virtualization** 2858
  Wenna Song *(Wuhan University)*, Jiang Ming *(University of Texas at Arlington)*,
  Lin Jiang *(Independent Researcher)*, Yi Xiang *(Wuhan University)*,
  Xuanchen Pan *(Wuhan Antiy Information Technology)*, Jianming Fu, Guojun Peng *(Wuhan University)*
- **One Glitch to Rule Them All: Fault Injection Attacks Against AMD's Secure Encrypted Virtualization** 2875
  Robert Buhren, Hans-Niklas Jacob, Thilo Krachenfels *(Technische Universität Berlin - SECT)*,
  Jean-Pierre Seifert *(Technische Universität Berlin - SECT & Fraunhofer SIT)*
- **RealSWATT: Remote Software-based Attestation for Embedded Devices under Realtime Constraints** 2890
  Sebastian Surminski, Christian Niesler *(University of Duisburg-Essen)*,
  Ferdinand Brasser *(Technical University Darmstadt)*, Lucas Davi *(University of Duisburg-Essen)*,
  Ahmad-Reza Sadeghi *(Technical University Darmstadt)*
- **PRIME+SCOPE: Overcoming the Observer Effect for High-Precision Cache Contention Attacks** 2906
  Antoon Purnal, Furkan Turan, Ingrid Verbauwhede *(imec-COSIC, KU Leuven)*
- **On the TOCTOU Problem in Remote Attestation** 2921
  Ivan De Oliveira Nunes *(Rochester Institute of Technology)*,
  Sashidhar Jakkamsetti *(University of California, Irvine)*,
  Norrathep Rattanavipanon *(Prince of Songkla University)*, Gene Tsudik *(University of California, Irvine)*
- **CROSSLINE: Breaking "Security-by-Crash" based Memory Isolation in AMD SEV** 2937
  Mengyuan Li *(The Ohio State University)*, Yinqian Zhang *(Southern University of Science and Technology)*,
  Zhiqiang Lin *(The Ohio State University)*

Session 11B: Zero Knowledge II

- **Zero Knowledge Static Program Analysis** 2951
  Zhiyong Fang *(Texas A&M University)*, David Darais *(Galois, Inc)*,
  Joseph P. Near *(University of Vermont)*, Yupeng Zhang *(Texas A&M University)*
- **zkCNN: Zero Knowledge Proofs for Convolutional Neural Network Predictions and Accuracy** 2968
  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)*
- **QuickSilver: Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field** 2986
  Kang Yang *(State Key Laboratory of Cryptology)*, Pratik Sarkar *(Boston University)*,
  Chenkai Weng, Xiao Wang *(Northwestern University)*
- **ZKCPlus: Optimized Fair-exchange Protocol Supporting Practical and Flexible Data Exchange** 3002
  Yun Li *(Institute for Network Sciences and Cyberspace of Tsinghua University)*,
  Cun Ye *(K-Orange/SECBIT Labs)*, Yuguang Hu, Ivring Morpheus, Yu Guo *(SECBIT Labs)*,
  Chao Zhang *(Institute for Network Science and Cyberspace of Tsinghua University)*,
  Yupeng Zhang *(Texas A&M University)*, Zhipeng Sun, Yiwen Lu *(SECBIT Labs)*,
  Haodi Wang *(Beijing Normal University)*
- **Limbo: Efficient Zero-knowledge MPCitH-based Arguments** 3022
  Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, Titouan Tanguy *(KU Leuven)*

Session 11C: Software Development and Analysis

- **"I need a better description": An Investigation Into User Expectations for Differential Privacy** 3037
  Rachel Cummings *(Columbia University)*, Gabriel Kaptchuk *(Boston University)*,
  Elissa M. Redmiles *(Max Planck Institute for Software Systems)*

- **An Inside Look into the Practice of Malware Analysis** 3053
  Miuyin Yong Wong, Matthew Landen, Manos Antonakakis,
  Douglas M. Blough *(Georgia Institute of Technology)*,
  Elissa M. Redmiles *(Max Planck Institute for Software Systems)*,
  Mustaque Ahamad *(Georgia Institute of Technology)*
- **The Effect of Google Search on Software Security: Unobtrusive Security Interventions via Content Re-ranking** 3070
  Felix Fischer, Yannick Stachelscheid, Jens Grossklags *(Technical University Munich)*
- **12 Angry Developers – A Qualitative Study on Developers' Struggles with CSP** 3085
  Sebastian Roth, Lea Theresa Gröber *(CISPA Helmholtz Center for Information Security & Saarland University)*,
  Michael Backes, Katharina Krombholz, Ben Stock *(CISPA Helmholtz Center for Information Security)*

Session 11D: Data Poisoning and Backdoor Attacks in ML

- **Subpopulation Data Poisoning Attacks** 3104
  Matthew Jagielski, Giorgio Severi, Niklas Pousette Harger, Alina Oprea *(Northeastern University)*
- **Hidden Backdoors in Human-Centric Language Models** 3123
  Shaofeng Li, Hui Liu, Tian Dong *(Shanghai Jiao Tong University)*,
  Benjamin Zi Hao Zhao *(The University of New South Wales & CSIRO-Data61)*,
  Minhui Xue *(The University of Adelaide)*, Haojin Zhu, Jialiang Lu *(Shanghai Jiao Tong University)*
- **Backdoor Pre-trained Models Can Transfer to All** 3141
  Lujia Shen, Shouling Ji, Xuhong Zhang, Jinfeng Li *(Zhejiang University)*, Jing Chen *(Wuhan University)*,
  Jie Shi, Chengfang Fang *(Huawei International, Singapore)*, Jianwei Yin *(Zhejiang University)*,
  Ting Wang *(The Pennsylvania State University)*
- **Feature-Indistinguishable Attack to Circumvent Trapdoor-Enabled Defense** 3159
  Chaoxiang He *(Huazhong University of Science and Technology)*, Bin Benjamin Zhu *(Microsoft Research Asia)*,
  Xiaojing Ma, Hai Jin, Shengshan Hu *(Huazhong University of Science and Technology)*
- **DetectorGuard: Provably Securing Object Detectors against Localized Patch Hiding Attacks** 3177
  Chong Xiang, Prateek Mittal *(Princeton University)*

Session 12A: Applications and Privacy of ML

- **DeepAID: Interpreting and Improving Deep Learning-based Anomaly Detection in Security Applications** 3197
  Dongqi Han, Zhiliang Wang, Wenqi Chen, Ying Zhong, Su Wang, Han Zhang, Jiahai Yang,
  Xingang Shi, Xia Yin *(Tsinghua University)*
- **Structural Attack against Graph Based Android Malware Detection** 3218
  Kaifa Zhao, Hao Zhou, Yulin Zhu, Xian Zhan, Kai Zhou, Jianfeng Li,
  Le Yu *(The Hong Kong Polytechnic University)*,
  Wei Yuan *(Huazhong University of Science and Technology)*,
  Xiapu Luo *(The Hong Kong Polytechnic University)*
- **PALMTREE: Learning an Assembly Language Model for Instruction Embedding** 3236
  Xuezixiang Li, Yu Qu, Heng Yin *(University of California, Riverside)*
- **A One-Pass Distributed and Private Sketch for Kernel Sums with Applications to Machine Learning at Scale** 3252
  Benjamin Coleman, Anshumali Shrivastava *(Rice University)*
- **COINN: Crypto/ML Codesign for Oblivious Inference via Neural Networks** 3266
  Siam Umar Hussain, Mojan Javaheripi, Mohammad Samragh, Farinaz Koushanfar
  (University of California, San Diego)

Session 12B: Analyzing Crashes and Incidents

- **Locating the Security Patches for Disclosed OSS Vulnerabilities with Vulnerability-Commit Correlation Ranking** 3282
  Xin Tan, Yuan Zhang, Chenyuan Mi, Jiajun Cao *(Fudan University)*,
  Kun Sun *(George Mason University)*, Yifan Lin, Min Yang *(Fudan University)*

- **Facilitating Vulnerability Assessment through PoC Migration** 3300
  Jiarun Dai, Yuan Zhang, Hailong Xu, Haiming Lyu, Zicheng Wu *(Fudan University)*,
  Xinyu Xing *(The Pennsylvania State University)*, Min Yang *(Fudan University)*
- **Igor: Crash Deduplication Through Root-Cause Clustering** 3318
  Zhiyuan Jiang, Xiyue Jiang *(National University of Defense Technology)*,
  Ahmad Hazimeh *(EPFL)*, Chaojing Tang *(National University of Defense Technology)*,
  Chao Zhang *(Tsinghua University)*, Mathias Payer *(EPFL)*
- **Validating the Integrity of Audit Logs Against Execution Repartitioning Attacks** 3337
  Carter Yagemann *(Georgia Institute of Technology)*,
  Mohammad A. Noureddine *(Rose-Hulman Institute of Technology)*,
  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)*
- **C3PO: Large-Scale Study Of Covert Monitoring of C&C Servers via Over-Permissioned Protocol Infiltration** 3352
  Jonathan Fuller, Ranjita Pai Kasturi, Amit Sikder, Haichuan Xu, Berat Arik, Vivek Verma,
  Ehsan Asdar, Brendan Saltaformaggio *(Georgia Institute of Technology)*

Session 12C: Traffic Analysis and Side Channels

- **New Directions in Automated Traffic Analysis** 3366
  Jordan Holland, Paul Schmitt *(Princeton University)*, Nick Feamster *(University of Chicago)*,
  Prateek Mittal *(Princeton University)*
- **Themis: Ambiguity-Aware Network Intrusion Detection based on Symbolic Model Comparison** 3384
  Zhongjie Wang, Shitong Zhu, Keyu Man, Pengxiong Zhu, Yu Hao, Zhiyun Qian,
  Srikanth V. Krishnamurthy *(University of California, Riverside)*,
  Tom La Porta *(The Pennsylvania State University)*, Michael J. De Lucia *(U.S. Army Research Laboratory)*
- **DNS Cache Poisoning Attack: Resurrections with Side Channels** 3400
  Keyu Man, Xin'an Zhou, Zhiyun Qian *(University of California, Riverside)*
- **Packet Scheduling with Optional Client Privacy** 3415
  Andrew Beams, Sampath Kannan *(University of Pennsylvania)*,
  Sebastian Angel *(University of Pennsylvania & Microsoft Research)*
- **Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis** 3431
  Chuanpu Fu *(Tsinghua University)*,
  Qi Li *(Tsinghua University & Beijing National Research Center for Information Science and Technology (BNRist))*,
  Meng Shen *(Beijing Institute of Technology)*,
  Ke Xu *(Tsinghua University & Beijing National Research Center for Information Science and Technology (BNRist), & Peng Cheng Laboratory)*

Session 12D: Decentralized Cryptographic Protocols

- **OpenSquare: Decentralized Repeated Modular Squaring Service** 3447
  Sri Aravinda Krishnan Thyagarajan *(Friedrich Alexander Universität Erlangen-Nuremberg)*,
  Tiantian Gong, Adithya Bhat, Aniket Kate *(Purdue University)*,
  Dominique Schröder *(Friedrich-Alexander Universität Erlangen-Nürnberg)*
- **Generalized Proof of Liabilities** 3465
  Yan Ji *(Cornell Tech & IC3)*, Konstantinos Chalkias *(Novi / Facebook)*
- **Mining in Logarithmic Space** 3487
  Aggelos Kiayias *(University of Edinburgh & IOHK)*,
  Nikos Leonardos, Dionysis Zindros *(University of Athens)*
- **RandPiper – Reconfiguration-Friendly Random Beacons with Quadratic Communication**. 3502
  Adithya Bhat *(Purdue University)*, Nibesh Shrestha *(Rochester Institute of Technology)*,
  Zhongtang Luo, Aniket Kate *(Purdue University)*, Kartik Nayak *(Duke University)*

Author Index 3525

ACM CCS 2021 Conference Organization

General Chairs:	Yongdae Kim (KAIST, Republic of Korea)
	Jong Kim (POSTECH, Republic of Korea)
Program Chairs:	Giovanni Vigna (University of California, Santa Barbara / VMware, USA)
	Elaine Shi (Carnegie Mellon University, USA)
Organizational Chair:	Jin Kwak (Ajou University, Republic of Korea)
Treasurer:	Changhoon Lee (SEOULTECH, Republic of Korea)
Registration Chair	Jongsung Kim (Kookmin University, Republic of Korea)
Web Chair:	Byoungyoung Lee (Seoul National University, Republic of Korea)
Publication Chairs:	Hyoungshick Kim (Sungkyunkwan University, Republic of Korea)
	Jin B. Hong (University of Western Australia, Australia)
Sponsorship Chairs:	Kyung Ho Lee (Korea University, Republic of Korea)
	David Mohaisen (University of Central Florida, USA)
	Kui Ren (ZheJiang University, China)
Student Travel Grant Chairs:	Yonghwi Kwon (University of Virginia, USA)
	Doowon Kim (University of Tennessee, USA)
Publicity Chairs:	Yeongjin Jang (Oregon State University, USA)
	Insu Yun (KAIST, Repubic of Korea)
Poster Chair:	Esha Ghosh (Microsoft Research, USA)
Workshop Chairs:	Michael Franz (University of California, Irvine, USA)
	Dokyung Song (Yonsei University, Republic of Korea)
Steering Committee:	Somesh Jha (Chair) (University of Wisconsin-Madison, USA)
	Rebecca Wright (Barnard College, USA)
	Carl Landwehr (George Washington University, USA)
	Trent Jaeger (Pennsylvania State University, USA)
	Stefan Savage (University of California-San Diego, USA)
	David Basin (ETH Zurich, Swiss)
Program Committee:	Abbas Razaghpanah (ICSI Research Scientist)
	Adam Doupe (Arizona State University)
	Adam Oest (PayPal)
	Ahmad Bashir (Google)
	Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Program Committee (continued): Albert Cheu (Georgetown University)
Alejandro Russo (Chalmers University of Technology)
Alessandra Scafuro (North Carolina State University)
Alexandra Dmitrienko (University of Wuerzburg)
Alexandros Kapravelos (North Carolina State University)
Alexandru Bardas (University of Kansas)
Alin Tomescu (VMware Research)
Alley Stoughton (Boston University)
Alvaro Cardenas (University of California, Santa Cruz)
Amir Rahmati (Stony Brook University)
Andrea Continella (University of Twente)
Andreas Zeller (CISPA Helmholtz Center for Information Security)
Andrei Sabelfeld (Chalmers University of Technology)
Andrew Baumann (Microsoft Research)
Ania Piotrowska (Nym Technologies)
Aniket Kate (Purdue University)
Anil Kurmus (IBM Research Europe - Zurich)
Anna Maria Mandalari (Imperial College, UK)
Antigoni Polychroniadou (J.P. Morgan AI Research)
Antonio Marcedone (Zoom Video Communications)
Anupam Das (North Carolina State University)
Arkady Yerukhimovich (George Washington University)
Arpita Patra (IISc Bangalore)
Arthur Gervais (Imperial College London)
Ashwin Machanavajjhala (Duke University)
Asia Slowinska (IBM Security)
Aurélien Francillon (EURECOM)
Aurore Fass (CISPA Helmholtz Center for Information Security)
Avishay Yanai (VMware Research)
Ben Livshits (Imperial College London)
Ben Stock (CISPA Helmholtz Center for Information Security)
Ben Y. Zhao (University of Chicago)
Benedikt Bünz (Stanford University)
Benjamin Fisch (Stanford University)
Bimal Viswanath (Virginia Tech)
Blase Ur (University of Chicago)
Bo Li (UIUC)
Bryan Ford (EPFL)
Carsten Baum (Aarhus University)
Catherine Meadows (US Naval Research Laboratory)
Chao Shen (Xi'an Jiaotong University)
Charalampos Papamanthou (University of Maryland)
Chen Yan (Zhejiang University)
Chris Hawblitzel (Microsoft Research)

Program Committee (continued):

Christina Ilvento (Harvard University)
Christopher Kruegel (University of California, Santa Barbara)
Dana Drachsler Cohen (Technion)
Danfeng Zhang (Penn State University)
Daniel Dubois (Northeastern University)
Daniel Genkin (University of Michigan)
Daniel Gruss (Graz University of Technology)
Daniel Holcomb (University of Massachusetts Amherst)
Daniel Kifer (Penn State)
Daniel Slamanig (AIT Austrian Institute of Technology)
Daniel Votipka (Tufts University)
David Barrera (Carleton Univeristy)
David Chisnall (Microsoft Research)
David Choffnes (Northeastern University)
David Heath (Georgia Institute of Technology)
Deepak Garg (Max Planck Institute for Software Systems)
Deian Stefan (UC San Diego)
Dominique Devriese (KU Leuven)
Doowon Kim (University of Tennessee, Knoxville)
Elaine Shi (Carnegie Mellon University)
Emmanuela Orsini (KU Leuven)
Engin Kirda (Northeastern University)
Eric Wustrow (University of Colorado Boulder)
Erik van der Kouwe (Vrije Universiteit Amsterdam)
Esha Ghosh (Microsoft Research)
Evgenios Kornaropoulos (George Mason University)
Ewa Syta (Trinity College)
Fan Zhang (Duke University)
Frank Li (Georgia Institute of Technology)
Frank Piessens (KU Leuven)
Frederico Araujo (IBM Research)
Gagandeep Singh (‘VMWare Research and UIUC)
Gang Wang (University of Illinois at Urbana-Champaign)
Gautam Kamath (University of Waterloo)
George Danezis (University College London)
Georgios Portokalidis (Stevens Institute of Technology)
Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security)
Giovanni Cherubin (Alan Turing Institute)
Giovanni Vigna (UC Santa Barbara and VMware)
Giulio Malavolta (Max Planck Institute for Security and Privacy)
Güliz Seray Tuncay (Google)
Hamed Okhravi (MIT Lincoln Laboratory)
Haojin Zhu (Shanghai Jiao Tong University)
Herbert Bos (Vrije Universiteit Amsterdam)

Program Committee (continued):

Hong-Sheng Zhou (Virginia Commonwealth University)
Ian Goldberg (University of Waterloo)
Ioana Boureanu (Univ. of Surrey, Surrey Centre for Cyber Security)
Irene Giacomelli (Protocol Labs)
Ittai Abraham (VMware Research)
Jason Polakis (University of Illinois at Chicago)
Jelena Mirkovic (USC)
Jeremiah Onaolapo (University of Vermont)
Jeyavijayan Rajendran (Texas A&M University)
Johannes Kinder (Bundeswehr University Munich)
Jon McCune (Google)
Jonathan Ullman (Northeastern University)
Joppe W. Bos (NXP Semiconductors)
Julian Loss (University of Maryland)
Jun Xu (Stevens Institute of Technology)
Kangjie Lu (University of Minnesota)
Kartik Nayak (Duke University)
Katharina Kohls (Radboud University)
Kaveh Razavi (ETH Zurich)
Kelsey Fulton (University of Maryland)
Klaus v. Gleissenthall (Vrije Universiteit Amsterdam)
Konrad Rieck (TU Braunschweig)
Kun Sun (George Mason University)
Lejla Batina (Radboud University)
Limin Jia (CMU)
Long Lu (Ant Group and Northeastern University)
Lorenzo Cavallaro (University College London)
Luca Invernizzi (Google)
Lucas Davi (University of Duisburg-Essen)
Lujo Bauer (Carnegie Mellon University)
Marcel Böhme (MPI-SP, Germany and Monash University, Australia)
Marco Guarnieri (IMDEA Software Institute)
Marco Patrignani (Cispa helmholtz center for information security)
Mariana Raykova (Google Inc.)
Mark Simkin (Aarhus University)
Martina Lindorfer (TU Wien)
Mathy Vanhoef (KU Leuven)
Matteo Maffei (TU Wien)
Mattijs Jonker (University of Twente)
Mayank Varia (Boston University)
Merve Sahin (SAP Security Research)
Micah Sherr (Georgetown University)
Michael Backes (CISPA Helmholtz Center for Information Security)
Michael Carl Tschantz (International Computer Science Institute)

Program Committee (continued):

Michael Coblenz (University of Maryland)
Michel van Eeten (Delft University of Technology)
Milad Nasr (UMASS)
Minhui (Jason) Xue (The University of Adelaide)
Mobin Javed (LUMS Pakistan)
Musard Balliu (KTH Royal Institute of Technology)
Muthuramakrishnan Venkitasubramaniam (University of Rochester)
Narseo Vallina-Rodriguez (IMDEA Networks/ICSI)
Neetesh Saxena (Cardiff University)
Neil Gong (Duke University)
Nele Mentens (Leiden University and KU Leuven)
Ni Trieu (Arizona State University)
Nick Nikiforakis (Stony Brook University)
Nikita Borisov (UIUC)
Nishanth Chandran (Microsoft Research, India)
Nuno Santos (INESC-ID / IST Universidade de Lisboa)
Oana Goga (CNRS)
Olga Ohrimenko (The University of Melbourne)
Patricia Arias Cabarcos (Paderborn University)
Patrick McDaniel (Penn State University)
Patrick Tague (Carnegie Mellon University)
Paul Pearce (Georgia Tech)
Pedro Moreno-Sanchez (IMDEA Software Institute)
Peter Rindal (Visa Research)
Peter Scholl (Aarhus University)
Peter Snyder (Brave Browser)
Phillipa Gill (Google/U. Massachusetts - Amherst)
Pin-Yu Chen (IBM Research AI)
Pramod Viswanath (UIUC)
Prateek Saxena (National University of Singapore)
Qi Alfred Chen (UC Irvine)
Qi Li (Tsinghua University)
Rahul Chatterjee (University of Wisconsin-Madison)
Rakesh Verma (University of Houston)
Ralf Sasse (ETH Zurich)
Reza Shokri (National University of Singapore (NUS))
Rishab Nithyanand (University of Iowa)
Roger Wattenhofer (ETH Zurich)
Ruben Martins (Carnegie Mellon University)
Ruoyu Fish Wang (Arizona State University)
Ryan Gerdes (Virginia Tech)
Sadia Afroz (ICSI, Avast)
Sajjad JJ Arshad (Google Inc.)
Sanchari Das (University of Denver)

Program Committee (continued):

Sarah Meiklejohn (University College London / Google)
Shiqing Ma (Rutgers University)
Shruti Tople (Microsoft Research)
Shuang Song (Google Research, Brain)
Siamak F. Shahandashti (University of York)
Simon Oya (University of Waterloo)
Simon Woo (Sungkyunkwan University)
Soo-Jin Moon (Google)
Sooel Son (KAIST)
Sophia Yakoubov (Aarhus University)
Srdjan Capkun (ETH Zurich)
Stefan Dziembowski (University of Warsaw)
Stefanie Roos (TU Delft)
Stefano Calzavara (Università Ca' Foscari Venezia)
Stéphanie Delaune (CNRS, Irisa)
Steve Lu (Stealth Software Technologies, Inc.)
Suman Jana (Columbia)
Tamara Rezk (INRIA Sophia-Antipolis)
Thomas Schneider (TU Darmstadt)
Tianhao Wang (Carnegie Mellon University and University of Virginia)
Timos Antonopoulos (Yale University)
Ting Wang (Penn State)
Tobias Fiebig (TU Delft)
Toby Murray (University of Melbourne)
Ulfar Erlingsson (Apple)
Umar Iqbal (The University of Iowa)
V.N. Venkatakrishnan (UIC)
Valeria Nikolaenko (Novi/Facebook)
Vasileios Kemerlis (Brown University)
Veelasha Moonsamy (Ruhr University Bochum)
Vincent Cheval (INRIA Paris)
Wei Meng (Chinese University of Hong Kong)
Wenbo Guo (The Pennsylvania State University)
Wenyuan Xu (Zhejiang University)
Xi He (University of Waterloo)
Xiangyu Zhang (Purdue University)
Xiao Wang (Northwestern University)
XiaoFeng Wang (Indiana University Bloomington)
Xiaoyu Ji (Zhejiang University)
Xinyu Xing (Pennsylvania State University)
Xuejia Lai (SJTU)
Yajin Zhou (Zhejiang University)
Yanchao Zhang (Arizona State University)
Yang Zhang (CISPA Helmholtz Center for Information Security)

Program Committee (continued):

Yanick Fratantonio (Cisco Talos)
Yier Jin (University of Florida)
Yinzhi Cao (Johns Hopkins University)
Yizheng Chen (University of California, Berkeley)
Yongdae Kim (KAIST)
Yousra Aafer (University of Waterloo)
Yuan Tian (University of Virginia)
Yupeng Zhang (Texas A&M University)
Z. Berkay Celik (Purdue University)
Z. Morley Mao (University of Michigan)
Ziming Zhao (University at Buffalo)

External reviewers:

Aaron Shim
Abhi Shelat
Abida Haque
Adam O’Neill
Adria Gascon
Akash Shah
Alexander Bienstock
Alexander Munch-Hansen
Alexander Sjösten
Alexander Spiegelman
Alexandros Zacharakis
Alina Oprea
Alwin Maier
Amos Treiber
Andreas Kogler
Andrew Miller
Ard Kastrati
Ariel Hamlin
Babak Falsafi
Behzad Abdolmaleki
Ben Hamlin
Benjamin Diamond
Benjamin Eriksson
Benny Pinkas
Binyi Chen
Blaine Hoak
Bo Feng
Calvin Huang
Carlos Gañán
Carmela Troncoso
Cedric Lauradoux
Chang Ge
Changhua Luo
Changhun Song
Chen Chen
Chen-Da Liu-Zhang
Chenghong Wang
Cheoljun Park
Chris Orsini
Christian Matt
Christian Niesler
Christian Weinert
Christine van Vredendaal
Clara Schneidewind
Claudio Canella
Constantin Catalin Dragan
Dalton Brucker-Hahn
Daniel Dubois
Daniel Escudero
Daniel Günther
Daniel Jost
David Malone
David Pujol
Debajyoti Das
Deevashwer Rathee
Diana Ghinea
Diego Aranha
Diego F. Aranha
Divya Gupta
Dmitry Kogan
Dongkwan Kim
Douglas Stebila
Duc Viet Le
Elissa M. Redmiles

External reviewers (continued):

Eran Lambooij
Eric Pauley
Erica Blum
Erkan Tairi
Erwin Quiring
Evgenios Kornaropoulos
Fang Song
Faysal Hossain Shezan
Felix Gunther
Finn de Ridder
Flavien Solt
Florian Tramer
Fnu Suya
Georges Alsankary
Gergely Acs
Gilad Stern
Habiba Farrukh
Hao Chen
Hao Chung
Hao Guo
Helen Möllering
Hila Dahari
Hongyan Chang
Hossein Yalame
Imane Fouad
Iyiola Emmanuel Olatunji
Jakub Sliwinski
James Mattei
Jens-Rene Giesen
Jiaheng Zhang
Jianfeng Chi
Jiayu Xu
Jiayuan Ye
Johannes Wikner
Johes Bater
Johes Bater
Jonathan Protzenko
Joppe W. Bos
Joseph Bonneau
Joshua Gancher
Kévin Huguenin
Kailani R. Jones
Kang Yang
Karl Knopf
Kevin Borgolte
Kexin Pei
Kiavash Satvat
Kirill Nikitin
Kristina Hostakova
Lukas Giner
Lukas Pirch
Lun Wang
Marc X. Makkes
Marcel Keller
Mariana Raykova
Mark Zhandry
Martin Schwarzl
Martin Strobel
Márton Bognár
Matthew Green
Matthew Jagielski
Matthew Lentz
Md Masoom Rabbani
Megumi Ando
Michael Rodler
Miguel Ambrona
Mike Rosulek
Mina Tahmasbi Arashloo
Mincheol Son
Mingxue Zhang
Mohamed Alzayat
Moritz Lipp
Mu Zhang
Nguyen Phong Hoang
Nikesh Shrestha
Nicolas Gailly
Oguzhan Ersoy
Oleksandr Tkachenko
Oliver Richter
Omer Shlomovits
Pablo Picazo-Sanchez
Paul Grubbs
Peiyao Sheng
Pengbin Feng
Penghui Li
Peter Kairouz
Pierre Laperdrix
Qiang Tang

External reviewers (continued):

Qiyang Song
Quinn Burke
Rahul Kande
Rahul Sharma
Ralf Kuesters
Rémi Hutin
Reza Mirzazade Farkhani
Richard Shin
Rigel Gjomemo
Rishabh Bhadauria
Rishav Chourasia
Roberto Guanciale
Ronald Thompson
Ruba Abu-Salma
Ruimin Sun
Ryan Rogers
Ryan Sheatsley
Sacha Servan-Schreiber
Sahar Mazloom
Sameer Wagh
Sangwook Bae
Satrajit Ghosh
Satwik Patnaik
Satya Lokam
Sebastian Ramacher
Sebastian Surminski
Shankari Jayasankaran
Shitong Zhu
Shu Wang
Shubhankar Mohapatra
Shufan Zhang
Songsong Liu
Sri Aravinda Krishnan Thyagarajan
Steve Wesemeyer
Stijn Pletinckx
Sutanu Ghosh
Syed Rafiul Hussain
Taejoong Chung
Tamjid Al Rahat
Tejaswi Nadahalli
Thang Hoang
Theophilus Benson
Tjerand Silde
Tobias Cloosters
Tom Yurek
Tu Le
Vadim Lyubashevsky
Valerio Cini
Varun Madathil
Vasudev Gohil
Wanrong Zhang
Waqar Aqeel
William Shand
Wutichai Chongchitmate
Xian Wu
Xiaoyuan Liu
Xinda Wang
Xiong Fan
Xu He
Xuejia Lai
Xueqing Li
Xunhua Wang
Yashashvi Dave
Ye Wang
Yinxi Liu
Yixin Sun
Yohan Beugin
Yue Duan
Yuhang Wu
Zhaokun Han
Zhenpeng Lin
Zhichuang Sun

ACM CCS 2021 Sponsor & Supporters

Sponsor: acm SIGSAC

Diamond Patron: HUAWEI

Platinum Patron: NSF

Gold Patrons:

蚂蚁集团 ANT GROUP | 蚂蚁安全实验室 ANT SECURITY LAB

Baidu 百度

FACEBOOK

IBM®

Samsung Research

vmware®

Silver Patrons:

AhnLab

Google

NAVER

TII Technology Innovation Institute

Bronze Patrons:

INPUT | OUTPUT

Institutional Supporters:

KOFST

KOREA TOURISM ORGANIZATION
www.visitkorea.or.kr

SEOUL METROPOLITAN GOVERNMENT

sto SEOUL TOURISM ORGANIZATION