# TABLE OF CONTENTS

**VOLUME 1**

## SESSION 1A: NETWORK SECURITY

Flexsealing BGP Against Route Leaks: Peerlock Active Measurement and Analysis

*Tyler McDaniel, Jared M. Smith, Max Schuchard*

A Devil of a Time: How Vulnerable is NTP to Malicious Timeservers?

*Yarin Perry, Neta Rozen-Schiff, Michael Schapira*

OblivSketch: Oblivious Network Measurement as a Cloud Service

*Shangqi Lai, Xingliang Yuan, Joseph Liu, Xun Yi, Qi Li, Dongxi Liu, Nepal Surya*

ROV++: Improved Deployable Defense against BGP Hijacking

*Reynaldo Morillo, Justin Furuness, Cameron Morris, James Breslin, Amir Herzberg, Bing Wang*

Trust the Crowd: Wireless Witnessing to Detect Attacks on ADS-B-Based Air-Traffic Surveillance

*Kai Jansen, Liang Niu, Nian Xue, Ivan Martinovic, Christina Pöpper*

## SESSION 1B: PROGRAM ANALYSIS 1

Towards Measuring Supply Chain Attacks on Package Managers for Interpreted Languages

*Ruian Duan, Omar Alrawi, Ranjita Pai Kasturi, Ryan Elder, Brendan Saltaformaggio, Wenke Lee*

Processing Dangerous Paths – On Security and Privacy of the Portable Document Format

*Jens Müller, Dominik Noss, Christian Mainka, Vladislav Mladenov, Jörg Schwenk*

XDA: Accurate, Robust Disassembly with Transfer Learning

*Kexin Pei, Jonas Guan, David Williams-King, Junfeng Yang, Suman Jana*

Shadow Attacks: Hiding and Replacing Content in Signed PDFs

*Christian Mainka, Vladislav Mladenov, Simon Rohlmann*

KUBO: Precise and Scalable Detection of User-triggerable Undefined Behavior Bugs in OS Kernel

*Changming Liu, Yaohui Chen, Long Lu*

## SESSION 1C: PRIVACY

Awakening the Web's Sleeper Agents: Misusing Service Workers for Privacy Leakage

*Soroush Karami, Panagiotis Ilia, Jason Polakis*

All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers

*Christoph Hagen, Christian Weinert, Christoph Sendner, Alexandra Dmitrienko, Thomas Schneider*

Improving Signal's Sealed Sender

*Ian Martiny, Gabriel Kaptchuk, Adam Aviv, Dan Roche, Eric Wustrow*
Tales of Favicons and Caches: Persistent Tracking in Modern Browsers ................................................................. 222
Konstantinos Solomos, John Kristoff, Chris Kanich, Jason Polakis

SESSION 2A: NETWORK POLICIES

Reining in the Web's Inconsistencies with Site Policy ............................................................................................ 241
Stefano Calzavara, Tobias Urban, Dennis Tatang, Marius Steffens, Ben Stock

From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR ............................................................................................................. 257
Chaoyi Lu, Baojun Liu, Yiming Zhang, Zhou Li, Fenglu Zhang, Haixin Duan, Yingliu, Joann Qiongna Chen, Jinjin Liang, Zaifeng Zhang, Shuang Hao, Min Yang

Understanding the Growth and Security Considerations of ECS .............................................................................. 275
Athanasios Kountouras, Panagiotis Kintis, Athanasios Avgetidis, Thomas Papastergiou, Charles Lever, Michalis Polychronakis, Manos Antonakakis

Mondrian: Comprehensive Inter-domain Network Zoning Architecture ........................................................................ 291
Jonghoon Kwon, Claude Hahni, Patrick Bamert, Adrian Perrig

SESSION 2B: PROGRAM ANALYSIS 2

Bringing Balance to the Force: Dynamic Analysis of the Android Application Framework ........................................ 307
Abdallah Dawoud, Sven Bugiel

SymQEMU: Compilation-based Symbolic Execution for Binaries ............................................................................. 325
Sebastian Poeplau, Aurélien Francillon

TASE: Reducing Latency of Symbolic Execution with Transactional Memory .......................................................... 343
Adam Humphries, Kartik Cating-Subramanian, Michael K. Reiter

Refining Indirect Call Targets at the Binary Level ..................................................................................................... 358
Sun Hyoung Kim, Cong Sun, Dongrui Zeng, Gang Tan

SESSION 2C: CRYPTO

Obfuscated Access and Search Patterns in Searchable Encryption ........................................................................... 376
Zhiwei Shang, Simon Oya, Andreas Peter, Florian Kerschbaum

More than a Fair Share: Network Data Remanence Attacks against Secret Sharing based Schemes ..................... 394
Leila Rashidi, Daniel Kostecki, Alexander James, Anthony Peterson, Majid Ghaderi, Samuel Jero, Cristina Nita-Rotaru, Hamed Okhravi, Reihaneh Safavi-Naini

Forward and Backward Private Conjunctive Searchable Symmetric Encryption .................................................... 408
Sikhar Patranabis, Debdeep Mukhopadhyay

Practical Non-Interactive Searchable Encryption with Forward and Backward Privacy ....................................... 426
Shi-Feng Sun, Ron Steinfeld, Shangqi Lai, Xingliang Yuan, Amin Sakzad, Joseph Liu, Surya Nepal, Dawu Gu
SESSION 3A: WEB SECURITY

Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks ........................................... 444
  Mohd Sabra, Anindya Maiti, Murtuza Jadliwala

Deceptive Deletions for Protecting Withdrawn Posts on Social Media Platforms ........................................... 462
  Mohsen Minaei, S Chandra Mouli, Mainack Mondal, Bruno Ribeiro, Aniket Kate

Who's Hosting the Block Party? Studying Third-Party Blockage of CSP and SRI ........................................... 480
  Marius Steffens, Marius Musch, Martin Johns, Ben Stock

To Err.Is Human: Characterizing the Threat of Unintended URLs in Social Media ......................................... 497
  Beliz Kaleli, Brian Kondracki, Manuel Egele, Nick Nikiforakis, Gianluca Stringhini

SerialDetector: Principled and Practical Exploration of Object Injection Vulnerabilities for the Web........... 512
  Mikhail Shcherbakov, Musard Balliu

SESSION 3B: MOBILE SECURITY

The Abuser Inside Apps: Finding the Culprit Committing Mobile Ad Fraud ........................................... 530
  Joongyum Kim, Jung-Hwan Park, Sooel Son

Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks ........................................... 546
  Xianghang Mi, Siyuan Tang, Zhengyi Li, Xiaojing Liao, Feng Qian, Xiaofeng Wang

Understanding Worldwide Private Information Collection on Android ........................................... 564
  Yun Shen, Pierre-Antoine Vervier, Gianluca Stringhini

On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices ........................................... 580
  Zeyu Lei, Yuhong Nan, Yanick Fratantonio, Antonio Bianchi

Preventing and Detecting State Inference Attacks on Android ........................................... 598
  Andrea Possemato, Dario Nisi, Yanick Fratantonio

SESSION 3C: BLOCKCHAINS

As Strong as Its Weakest Link: How to Break Blockchain DApps at RPC Service ........................................... 616
  Kai Li, Jiaqi Chen, Xianghong Liu, Yuzhe Tang, Xiaofeng Wang, Xiapu Luo

RandRunner: Distributed Randomness from Trapdoor VDFs with Strong Uniqueness ........................................... 634
  Philipp Schindler, Aljosha Judmayer, Markus Hittmeir, Nicholas Stifter, Edgarweippl

LaKSA: A Probabilistic Proof-of-Stake Protocol ........................................... 652
  Daniel Reisbergen, Pawel Szalachowski, Junming Ke, Zengpeng Li, Jianying Zhou

SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning ........................................... 670
  Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramèr, Giulia Fanti, Ari Juels

Bitcontracts: Supporting Smart Contracts in Legacy Blockchains ........................................... 688
  Karl Wüst, Loris Diana, Kari Kostiainen, Ghassan Karame, Sinisa Matetic, Srdjan Capkun
SESSION 4A: NETWORK PROTOCOLS

QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit ............ 706
James Pavur, Martin Strohmeier, Vincent Lenders, Ivan Martinovic

A Formal Analysis of the FIDO UAF Protocol ................................................................. 723
Haonan Feng, Hui Li, Xuesong Pan, Ziming Zhao

PHOENIX: Device-Centric Cellular Network Protocol Monitoring using Runtime Verification ............ 738
Mitziu Echeverria, Zeeshan Ahmed, Bincheng Wang, M. Fareed Arif, Syed Rafiulhussain,
Omar Chowdhury

SESSION 4B: SIDE-CHANNELS AND SPECULATION

Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an
Electromagnetic Side Channel ................................................................. 792
Zhuoran Liu, Niels Samwel, Léo Weissbart, Zhengyu Zhao, Dirk Lauret, Lejlabatina, Martha Larson

Rosita: Towards Automatic Elimination of Power-Analysis Leakage in Ciphers ............................... 807
Madura A. Shelton, Niels Samwel, Lejla Batina, Francesco Regazzoni, Markus Wagner,
Yuval Yarom

Hunting the Haunter — Efficient Relational Symbolic Execution for Spectre with Haunted RelSE ........ 824
Lesly-Ann Daniel, Sébastien Bardin, Tamara Rezk

SpecTaint: Speculative Taint Analysis for Discovering Spectre Gadgets ........................................ 841
Zhenxiao Qi, Qian Feng, Yueqiang Cheng, Mengjia Yan, Peng Li, Heng Yin, Tao Wei

SESSION 4C: MALWARE AND CYBER-CRIME

Understanding and Detecting International Revenue Share Fraud ............................................. 855
Merve Sahin, Aurélien Francillon

Detection ................................................................. 871
Jiayun Xu, Yingjiu Li, Robert H. Deng

MINOS: A Lightweight Real-Time Cryptojacking Detection System ........................................... 885
Faraz Naseem, Ahmet Aris, Leonardo Babun, Ege Tekiner, A. Selcuk Uluagac

Does Every Second Count? Time-based Evolution of Malware Behavior in Sandboxes ................. 900
Alexander Küchler, Alessandro Mantovani, Yufei Han, Leyla Bilge, Davide Balzarotti
SESSION 5A: “SMART” HOME

Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem ................................................. 918
Christopher Lentzsch, Sheel Jayesh Shah, Benjamin Andow, Martin Degeling, Anupam Das,
William Enck

IoTSafe: Enforcing Safety and Security Policy with Real IoT Physical Interaction Discovery ...................... 936
Wenbo Ding, Hongxin Hu, Long Cheng

PFirewall: Semantics-Aware Customizable Data Flow Control for Smart Home Privacy Protection ............... 954
Haotian Chi, Qiang Zeng, Xiaojiang Du, Lannan Luo

EarArray: Defending against DolphinAttack via Acoustic Attenuation.............................................................. 972
Guoming Zhang, Xiaoyu Ji, Xinfeng Li, Gang Qu, Wenyuan Xu

SESSION 5B: SOFTWARE DEFENSES

POPOP and PUSH: Demystifying and Defending against (Mach) Port-oriented Programming......................... 986
Min Zheng, Xiaolong Bai, Yajin Zhou, Chao Zhang, Fuping Qu

Доверій, но перевірій: SFI safety for native-compiled Wasm ........................................................................... 1003
Evan Johnson, David Thien, Yousef Alhessi, Shravan Narayan, Fraser Brown, Sorin Lerner,
Tyler McMullen, Stefan Savage, Deian Stefan

Detecting Kernel Memory Leaks in Specialized Modules with Ownership Reasoning .................................... 1019
Navid Emamdoost, Qiushi Wu, Kangjie Lu, Stephen McCamant

SESSION 5C: MACHINE LEARNING

Let's Stride Blindfolded in a Forest: Sublinear Multi-Client Decision Trees Evaluation ..................................... 1037
Jack P. K. Ma, Raymond K. H. Tai, Yongjun Zhao, Sherman S. M. Chow

Practical Blind Membership Inference Attack via Differential Comparisons ...................................................... 1055
Bo Hui, Yuchen Yang, Haolin Yuan, Philippe Burlina, Neil Zhenqiang Gong, Yinzhicao

GALA: Greedy Computation for Linear Algebra in Privacy-Preserved Neural Networks .............................. 1072
Qiao Zhang, Chunsheng Xin, Hongyi Wu

FARE: Enabling Fine-grained Attack Categorization under Low-quality Labeled Data ............................... 1088
Junjie Liang, Wenbo Guo, Tongbo Luo, Vasant Honavar, Gang Wang, Xinyu Xing

SESSION 6A: FUZZING

PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles ...................................................................................... 1106
Hyungsuk Kim, Muslum Ozgur Ozmen, Antonio Bianchi, Z. Berkay Celik, Dongyan Xu

Favocado: Fuzzing Binding Code of JavaScript Engines Using Semantically Correct TestCases .................... 1124
Sung Ta Dinh, Haehyun Cho, Kyle Martin, Adam Oest, Yihui Zeng, Alexandros Kapravelos,
Tiffany Bao, Ruoyu Wang

WINNIE: Fuzzing Windows Applications with Harness Synthesis and Fast Cloning ..................................... 1139
Jinho Jung, Stephen Tong, Hong Hu, Jungwon Lim, Yonghwi Jin, Taesoo Kim
Reinforcement Learning-based Hierarchical Seed Scheduling for Greybox Fuzzing

Jinghan Wang, Chengyu Song, Heng Yin

SESSION 6B: EMBEDDED SECURITY

Evading Voltage-Based Intrusion Detection on Automotive CAN

Rohit Bhatia, Vireshwar Kumar, Khaled Serag, Z. Berkay Celik, Mathias Payer, Dongyan Xu

HERA: Hotpatching of Embedded Real-time Applications

Christian Niesler, Sebastian Surminski, Lucas Davi

From Library Portability to Para-rehosting: Natively Executing Microcontroller Software on Commodity Hardware

Wenqiang Li, Le Guan, Jingqiang Lin, Jiameng Shi, Fengjun Li

BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols

Eunsoo Kim, Dongkwan Kim, Cheoljun Park, Insu Yun, Yongdae Kim

SESSION 6C: FEDERATED LEARNING AND POISONING ATTACKS

POSEIDON: Privacy-Preserving Federated Neural Network Learning

Sinem Sav, Apostolos Pyrgelis, Juan Ramón Troncoso-Pastoriza, David Froelicher, Jean-Philippe Bossuyt, João Sa Sousa, Jean-Pierre Hubaux

FLTrust: Byzantine-robust Federated Learning via Trust Bootstrapping

Xiaoyu Cao, Minghong Fang, Jia Liu, Neil Zhenqiang Gong

Manipulating the Byzantine: Optimizing Model Poisoning Attacks and Defenses for Federated Learning

Virat Shejwalkar, Amir Houmansadr

Data Poisoning Attacks to Deep Learning Based Recommender Systems

Hai Huang, Jiaming Mu, Neil Zhenqiang Gong, Qi Li, Bin Liu, Mingwei Xu

SESSION 7A: FORENSICS AND AUDITS

C²SR Cybercrime Scene Reconstruction for Post-mortem Forensic Analysis

Yonghwi Kwon, Weihang Wang, Jinho Jung, Kyu Hyung Lee, Roberto Perdisci

ALchemist: Fusing Application and Audit Logs for Precise Attack Provenance without Instrumentation

Le Yu, Shiqing Ma, Zhuo Zhang, Guanhong Tao, Xiangyu Zhang, Dongyan Xu, Vincent E. Urias, Han Wei Lin, Gabriela Ciocarlie, Vinod Yegneswaran, Ashish Gehani

WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics

Jun Zeng, Zheng Leong Chua, Yinfang Chen, Kaihang Ji, Zhenkai Liang, Jian Mao

SESSION 7B: TRUSTED COMPUTING

DOVE: A Data-Oblivious Virtual Environment

Hyun Bin Lee, Tushar Jois, Christopher Fletcher, Carl A. Gunter
CHANCEL: Efficient Multi-client Isolation Under Adversarial Programs ................................................. 1384
  Adil Ahmad, Juhee Kim, Jaebaek Seo, Insik Shin, Pedro Fonseca, Byoungyoung Lee

Emilia: Catching Iago in Legacy Code ........................................................................................................... 1402
  Rongchen Cui, Lianying Zhao, David Lie

SESSION 7C: MACHINE LEARNING APPLICATIONS

CV-Inspector: Towards Automating Detection of Adblock Circumvention ......................................................... 1419
  Hieu Le, Athina Markopoulou, Zubair Shafiq

FlowLens: Enabling Efficient Flow Classification for ML-based Network Security Applications ................. 1437
  Diogo Barradas, Nuno Santos, Luis Rodrigues, Salvatore Signorello, Fernando M. V. Ramos,
  André Madeira

PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps .................................................. 1455
  Sebastian Zimmeck, Rafael Goldstein, David Baraka

Towards Understanding and Detecting Cyberbullying in Real-world Images .............................................. 1473
  Nishant Vishwamitra, Hongxin Hu, Feng Luo, Long Cheng

ADDITIONAL PAPERS

PhantomCache: Obfuscating Cache Conflicts with Localized Rendomization ............................................. 1491
  Qinhan Tan, Zhihua Zeng, Kai Bu, Kui Ren

UISCOPE: Accurate, Instrumentation-free, and Visible Attack Investigation for GUI Applications .......... 1508
  Runqing Yang, Shiqing Ma, Haitao Xu, Xiangyu Zhang, Yan Chen

SODA: A Generic Online Detection Framework for Smart Contracts ...................................................... 1526
  Ting Chen, Rong Cao, Ting Li, Xiapu Luo, Guofei Gu, Yufei Zhang, Zhou Liao, Hang Zhu,
  Gang Chen, Zheyuan He, Yuxing Tang, Xiaodong Lin, Xiaosong Zhang

Author Index