ACM Conference on Computer and Communications Security

CCS 2017 - Accepted Papers

The following papers have been accepted to the 24th ACM Conference on Computer and Communications Security (151 papers accepted out of 836 submissions). All papers are available using the [PDF] link. (If the author also posted an open version of the paper, it is available using the [Paper] link.)

List By Authors · **Institutions** · **Papers by Session** · **Papers by Topic** · **Award Finalists** · **Available Papers** · **Artifacts**

(Ordered by Conference Session)

DUPLO: Unifying Cut-and-Choose for Garbled Circuits [PDF] [Paper] [Artifact] (A1)	Vladimir Kolesnikov, Jesper Buus Nielsen, Mike Rosulek, Ni Trieu, Roberto Trifiletti
Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation [PDF] [Paper] [Artifact] (A1) ★	Xiao Wang, Samuel Ranellucci, Jonathan Katz
Global-Scale Secure Multiparty Computation [PDF] [Paper] [Artifact] (A1)	Xiao Wang, Samuel Ranellucci, Jonathan Katz
Hearing Your Voice Is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication [PDF] (A2)	Linghan Zhang, Sheng Tan, Jie Yang
VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration [PDF] (A2)	Jian Liu, Chen Wang, Yingying Chen, Nitesh Saxena

Presence Attestation: The Missing Link In Dynamic Trust Bootstrapping [PDF] (A2)	Zhangkai Zhang, Xuhua Ding, Gene Tsudik, Jinhua Cui, Zhoujun Li
DolphinAttack: Inaudible Voice Commands [PDF] [Paper] (A3) ★	Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, Wenyuan Xu
Evading Classifiers by Morphing in the Dark [PDF] (A3)	Hung Dang, Yue Huang, Ee-Chien Chang
MagNet: a Two-Pronged Defense against Adversarial Examples [PDF] [Paper] (A3)	Dongyu Meng, Hao Chen
Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers [PDF] (A4)	Meng Luo, Oleksii Starov, Nima Honarmand, Nick Nikiforakis
Deterministic Browser [PDF] [Paper] [Artifact] (A4)	Yinzhi Cao, Zhanhao Chen, Song Li, Shujiang Wu
Most Websites Don't Need to Vibrate: A Cost-Benefit Approach to Improving Browser Security [PDF] [Paper] (A4)	Peter Snyder, Cynthia Taylor, Chris Kanich
Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin [PDF] [Paper] (A5)	Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Vasserman, Yongdae Kim
Betrayal, Distrust, and Rationality: Smart Counter-Collusion Contracts for Verifiable Cloud Computing [PDF] [Paper] [Artifact] (A5)	Changyu Dong, Yilei Wang, Amjad Aldweesh, Patrick McCorry, Aad van Moorsel
Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for Services [PDF] [Paper] [Artifact] (A5)	Matteo Campanelli, Rosario Gennaro, Steven Goldfeder, Luca Nizzardo
Pool: Scalable On-Demand Secure Computation Service Against Malicious Adversaries [PDF] [Paper] [Artifact] (B1)	Ruiyu Zhu, Yan Huang, Darion Cassel
A Framework for Constructing Fast MPC over Arithmetic Circuits with Malicious Adversaries and an Honest-Majority [PDF] [Paper] (B1)	Yehuda Lindell, Ariel Nof

Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case [PDF] [Paper] (B1)	Nishanth Chandran, Juan Garay, Payman Mohassel, Satyanarayana Vusirikala
Let's go in for a closer look: Observing passwords in their natural habitat [PDF] (B2)	Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Alain Forget
Why Do Developers Get Password Storage Wrong? A Qualitative Usability Study [PDF] [Paper] (B2)	Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, Matthew Smith
The TypTop System: Personalized Typo-tolerant Password Checking [PDF] [Paper] [Artifact] (B2)	Rahul Chatterjee, Joanne Woodage, Yuval Pnueli, Anusha Chowdhury, Thomas Ristenpart
Rise of the HaCRS: Augmenting Autonomous Cyber Reasoning Systems with Human Assistance [PDF] (B3)	Yan Shoshitaishvili, Michael Weissbacher, Lukas Dresel, Christopher Salls, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna
Neural Network-based Graph Embedding for Cross-Platform Binary Code Similarity Detection [PDF] [Paper] (B3)	Xiaojun Xu, Chang Liu, Qian Feng, Heng Yin, Le Song, Dawn Song
RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking [PDF] (B3)	Yang Ji, Sangho Lee, Evan Downing, Weiren Wang, Mattia Fazzini, Taesoo Kim, Alessandro Orso, Wenke Lee
Synthesis of Probabilistic Privacy Enforcement [PDF] [Artifact] (B4)	Martin Kucera, Petar Tsankov, Timon Gehr, Marco Guarnieri, Martin Vechev
A Type System for Privacy Properties [PDF] [Paper] [Artifact] (B4)	Véronique Cortier, Niklas Grimm, Joseph Lallemand, Matteo Maffei
Generating Synthetic Decentralized Social Graphs with Local Differential Privacy [PDF] (B4)	Zhan Qin, Yin Yang, Ting Yu, Xiaokui Xiao, Issa Khalil, Kui Ren

Revive: Rebalancing Off-Blockchain Payment Networks [PDF] [Artifact] (B5)	Rami Khalil, Arthur Gervais
Concurrency and Privacy with Payment-Channel Networks [PDF] [Paper] (B5)	Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Srivatsan Ravi
Bolt: Anonymous Payment Channels for Decentralized Currencies [PDF] (B5)	Matthew Green, Ian Miers
S3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing [PDF] [Paper] [Artifact] (C1)	Thang Hoang, Ceyhun D. Ozkaptan, Attila A. Yavuz, Jorge Guajardo, Tam Nguyen
Deterministic, Stash-Free Write-Only ORAM [PDF] [Paper] [Artifact] (C1)	Daniel S. Roche, Adam J. Aviv, Seung Geol Choi, Travis Mayberry
Scaling ORAM for Secure Computation [PDF] [Paper] [Artifact] (C1) ★	Jack Doerner, abhi shelat
Don’t Let One Rotten Apple Spoil the Whole Barrel: Towards Automated Detection of Shadowed Domains [PDF] (C2)	Daiping Liu, Zhou Li, Kun Du, Haining Wang, Baojun Liu, Haixin Duan
Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting [PDF] [Paper] (C2)	Samaneh Tajalizadehkhoob, Tom van Goethem, Maciej Korczyński, Arman Noroozian, Rainer Böhme, Tyler Moore, Wouter Joosen, Michel van Eeten
Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse [PDF] [Paper] (C2)	Panagiotis Kintis, Najmeh Miramirkhani, Charles Lever, Yizheng Chen, Rosa Romero-Gómez, Nikolaos Pitropakis, Nick Nikiforakis, Manos Antonakakis
Machine Learning Models that Remember Too Much [PDF] (C3)	Congzheng Song, Thomas Ristenpart, Vitaly Shmatikov

Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning [PDF] [Paper] (C3)	Briland Hitaj, Giuseppe Ateniese, Fernando Perez-Cruz
Oblivious Neural Network Predictions via MiniONN transformations [PDF] [Paper] (C3)	Jian Liu, Mika Juuti, Yao Lu, N. Asokan
Verifying Security Policies in Multi-agent Workflows with Loops [PDF] [Paper] [Artifact] (C4)	Bernd Finkbeiner, Christian Müller, Helmut Seidl, Eugen Zalinescu
Attribute-Based Encryption in the Generic Group Model: Automated Proofs and New Constructions [PDF] (C4)	Miguel Ambrona, Gilles Barthe, Romain Gay, Hoeteck Wee
FAME: Fast Attribute-based Message Encryption [PDF] [Paper] [Artifact] (C4)	Shashank Agrawal, Melissa Chase
Practical UC-Secure Delegatable Credentials with Attributes and Their Application to Blockchain [PDF] (C5)	Jan Camenisch, Manu Drijvers, Maria Dubovitskaya
Solidus: Confidential Distributed Ledger Transactions via PVORM [PDF] [Paper] (C5)	Ethan Cecchetti, Fan Zhang, Yan Ji, Ahmed Kosba, Ari Juels, Elaine Shi
Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards [PDF] (C5)	Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, Ian Miers
5Gen-C: Multi-input Functional Encryption and Program Obfuscation for Arithmetic Circuits [PDF] [Artifact] (D1)	Brent Carmer, Alex J. Malozemoff, Mariana Raykova
Iron: Functional Encryption using Intel SGX [PDF] [Paper] (D1) ★	Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, Sergey Gorbunov
Implementing BP-Obfuscation Using Graph-Induced Encoding [PDF] [Paper] (D1)	Shai Halevi, Tzipora Halevi, Victor Shoup, Noah Stephens-Davidowitz

AUTHSCOPE: Towards Automatic Discovery of Vulnerable Access Control in Online Services [PDF] (D2)	Chaoshun Zuo, Qingchuan Zhao, Zhiqiang Lin
Mass Discovery of Android Traffic Imprints through Instantiated Partial Execution [PDF] (D2)	Yi Chen, Wei You, Yeonjoon Lee, Kai Chen, XiaoFeng Wang, Wei Zou
Unleashing the Walking Dead: Understanding Cross-App Remote Infections on Mobile WebViews [PDF] (D2)	Tongxin Li, Xueqiang Wang, Mingming Zha, Kai Chen, XiaoFeng Wang, Luyi Xing, Xiaolong Bai, Nan Zhang, Xinhui Han
May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519 [PDF] [Paper] (D3)	Daniel Genkin, Luke Valenta, Yuval Yarom
Stacco: Differentially Analyzing Side-Channel Traces for Detecting SSL/TLS Vulnerabilities in Secure Enclaves [PDF] [Paper] (D3)	Yuan Xiao, Mengyuan Li, Sanchuan Chen, Yinqian Zhang
Precise Detection of Side-Channel Vulnerabilities using Quantitative Cartesian Hoare Logic [PDF] (D3)	Jia Chen, Yu Feng, Isil Dillig
Better Than Advertised: Improved Collision-Resistance Guarantees for MD-Based Hash Functions [PDF] (D4)	Mihir Bellare, Joseph Jaeger, Julia Len
Generic Semantic Security against a Kleptographic Adversary [PDF] (D4)	Alexander Russell, Qiang Tang, Moti Yung, Hong-Sheng Zhou
Defending Against Key Exfiltration: Efficiency Improvements for Big-Key Cryptography via Large-Alphabet Subkey Prediction [PDF] (D4)	Mihir Bellare, Wei Dai
Client-side Name Collision Vulnerability in the New gTLD Era: A Systematic Study [PDF] [Paper] (D5)	Qi Alfred Chen, Matthew Thomas, Eric Osterweil, Yulong Cao, Jie You, Z. Morley Mao

The Wolf of Name Street: Hijacking Domains Through Their Nameservers [PDF] [Paper] (D5)	Thomas Vissers, Timothy Barron, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis
Faulds: A Non-Parametric Iterative Classifier for Internet-Wide OS Fingerprinting [PDF] [Paper] (D5)	Zain Shamsi, Daren B.H. Cline, Dmitri Loguinov
T/Key: Second-Factor Authentication From Secure Hash Chains [PDF] [Paper] (E1)	Dmitry Kogan, Nathan Manohar, Dan Boneh
Practical Graphs for Optimal Side-Channel Resistant Memory-Hard Functions [PDF] [Paper] [Artifact] (E1)	Joel Alwen, Jeremiah Blocki, Ben Harsha
Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation [PDF] [Paper] (E1) ★	Shay Gueron, Yehuda Lindell
The ART of App Compartmentalization: Compiler-based Library Privilege Separation on Stock Android [PDF] (E2)	Jie Huang, Oliver Schranz, Sven Bugiel, Michael Backes
Vulnerable Implicit Service: A Revisit [PDF] (E2)	Lingguang Lei, Yi He, Kun Sun, Jiwu Jing, Yuewu Wang, Qi Li, Jian Weng
A Stitch in Time: Supporting Android Developers in Writing Secure Code [PDF] (E2)	Duc Cuong Nguyen, Dominik Wermke, Yasemin Acar, Michael Backes, Charles Weir, Sascha Fahl
Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers [PDF] (E3)	Mohammad A. Islam, Shaolei Ren, Adam Wierman
Watch Me, but Don’t Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations [PDF] [Paper] (E3)	Yi Han, Sriharsha Etigowni, Hua Liu, Saman Zonouz, Athina Petropulu
Viden: Attacker Identification on In-Vehicle Networks [PDF] [Paper] (E3)	Kyong-Tak Cho, Kang G. Shin

Practical Attacks Against Graph-based Clustering [PDF] [Paper] (E4)	Yizheng Chen, Yacin Nadji, Athanasios Kountouras, Fabian Monrose, Roberto Perdisci, Manos Antonakakis, Nikolaos Vasiloglou
Automated Crowdturfing Attacks and Defenses in Online Review Systems [PDF] [Paper] (E4)	Yuanshun Yao, Bimal Viswanath, Jenna Cryan, Haitao Zheng, Ben Y. Zhao
POISED: Spotting Twitter Spam Off the Beaten Paths [PDF] [Paper] (E4)	Shirin Nilizadeh, François Labrèche, Alireza Sadighian, Ali Zand, José Fernandez, Christopher Kruegel, Gianluca Stringhini, Giovanni Vigna
Practical Secure Aggregation for Privacy-Preserving Machine Learning [PDF] [Paper] (E5)	Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, Karn Seth
Use Privacy in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs [PDF] [Paper] [Artifact] (E5)	Anupam Datta, Matthew Fredrikson, Gihyuk Ko, Piotr Mardziel, Shayak Sen
SGX-BigMatrix: A Practical Encrypted Data Analytic Framework With Trusted Processors [PDF] (E5)	Fahad Shaon, Murat Kantarcioglu, Zhiqiang Lin, Latifur Khan
Malicious-Secure Private Set Intersection via Dual Execution [PDF] [Paper] [Artifact] (F1)	Peter Rindal, Mike Rosulek
Fast Private Set Intersection from Homomorphic Encryption [PDF] [Paper] (F1)	Hao Chen, Kim Laine, Peter Rindal
Practical Multi-party Private Set Intersection from Symmetric-Key Techniques [PDF] [Paper] [Artifact] (F1)	Vladimir Kolesnikov, Naor Matania, Benny Pinkas, Mike Rosulek, Ni Trieu
Detecting Structurally Anomalous Logins Within Enterprise Networks [PDF] (F2)	Hossein Siadati, Nasir Memon

DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning [PDF] (F2)	Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar
Predicting the Risk of Cyber Incidents [PDF] (F2)	Leyla Bilge, Yufei Han, Matteo Dell'Amico
Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [PDF] [Paper] (F3) ★	Mathy Vanhoef, Frank Piessens
CCCP: Closed Caption Crypto Phones to Resist MITM Attacks, Human Errors and Click-Through [PDF] (F3)	Maliheh Shirvanian, Nitesh Saxena
No-Match Attacks and Robust Partnering Definitions — Defining Trivial Attacks for Security Protocols is Not Trivial [PDF] [Paper] (F3)	Yong Li, Sven Schäge
Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR [PDF] [Paper] (F4)	Syed Mahbub Hafiz, Ryan Henry
PeGaSus: Data-Adaptive Differentially Private Stream Processing [PDF] (F4)	Yan Chen, Ashwin Machanavajjhala, Michael Hay, Gerome Miklau
Composing Differential Privacy and Secure Computation: A case study on scaling private record linkage [PDF] [Paper] (F4)	Xi He, Ashwin Machanavajjhala, Cheryl Flynn, Divesh Srivastava
Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors [PDF] (F5)	Mustafa Emre Acer, Emily Stark, Adrienne Porter Felt, Sascha Fahl, Radhika Bhargava, Bhanu Dev, Matt Braithwaite, Ryan Sleevi, Parisa Tabriz
Data breaches, phishing, or malware? Understanding the risks of stolen credentials [PDF] (F5)	Kurt Thomas, Frank Li, Ali Zand, Jake Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, Dan Margolis, Vern Paxson, Elie Bursztein

Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI [PDF] (F5)	Doowon Kim, Bum Jun Kwon, Tudor Dumitraş
Forward Secure Dynamic Searchable Symmetric Encryption with Efficient Updates [PDF] (G1)	Kee Sung Kim, Minkyu Kim, Dongsoo Lee, Je Hong Park, Woo-Hwan Kim
Forward and Backward Private Searchable Encryption from Constrained Cryptographic Primitives [PDF] [Paper] [Artifact] (G1)	Raphael Bost, Brice Minaud, Olga Ohrimenko
Economic Factors of Vulnerability Trade and Exploitation: Empirical evidence from a prominent Russian cybercrime market [PDF] [Paper] (G2)	Luca Allodi
Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research [PDF] [Paper] [Artifact] (G2)	Alexander Gamero-Garrido, Stefan Savage, Kirill Levchenko, Alex C. Snoeren
Identity-Based Format-Preserving Encryption [PDF] (G3)	Mihir Bellare, Viet Tung Hoang
Standardizing Bad Cryptographic Practice - A teardown of the IEEE standard for protecting electronic-design intellectual property [PDF] (G3)	Animesh Chhotaray, Adib Nahiyan, Thomas Shrimpton, Domenic J Forte, Mark Tehranipoor
New Techniques for Structural Batch Verification in Bilinear Groups with Applications to Groth-Sahai Proofs [PDF] [Paper] (G4)	Gottfried Herold, Max Hoffmann, Michael Klooß , Carla Ràfols, Andy Rupp
Practical Quantum-Safe Voting from Lattices [PDF] (G4)	Rafael del Pino, Vadim Lyubashevsky, Gregory Neven, Gregor Seiler
A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components [PDF] [Paper] [Artifact] (G5)	Vasilios Mavroudis, Andrea Cerulli, Petr Svenda, Dan Cvrcek, Dusan Klinec, George Danezis

Provably-Secure Logic Locking: From Theory To Practice [PDF] (G5)	Muhammad Yasin, Abhrajit Sengupta, Mohammed Thari Nabeel, Mohammed Ashraf, Jeyavijayan (JV) Rajendran, Ozgur Sinanoglu
The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli [PDF] [Artifact] (H1) ★	Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec, Vashek Matyas
Algorithm Substitution Attacks from a Steganographic Perspective [PDF] [Paper] (H1)	Sebastian Berndt, Maciej Liskiewicz
On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs [PDF] [Paper] (H1) ★	Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, Christian Boit
The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later [PDF] [Paper] [Artifact] (H2)	Victor van der Veen, Dennis Andriesse, Manolis Stamatogiannakis, Xi Chen, Herbert Bos, Cristiano Giuffrida
Capturing Malware Propagations with Code Injections and Code-Reuse attacks [PDF] (H2)	David Korczynski, Heng Yin
Code-reuse attacks for the Web: Breaking Cross-Site Scripting Mitigations via Script Gadgets [PDF] (H2)	Sebastian Lekies, Krzysztof Kotowicz, Samuel Groß , Eduardo Vela, Martin Johns
Tail Attacks on Web Applications [PDF] (H3)	Huasong Shan, Qingyang Wang, Calton Pu
Rewriting History: Changing the Archived Web from the Present [PDF] [Paper] [Artifact] (H3)	Ada Lerner, Tadayoshi Kohno, Franziska Roesner
Deemon: Detecting CSRF with Dynamic Analysis and Property Graphs [PDF] [Paper] (H3)	Giancarlo Pellegrino, Martin Johns, Simon Koch, Michael Backes, Christian Rossow

A Comprehensive Symbolic Analysis of TLS 1.3 [PDF] [Paper] [Artifact] (H4)	Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, Thyla van der Merwe
HACL: A Verified Modern Cryptographic Library* [PDF] [Paper] [Artifact] (H4)	Jean-Karim Zinzindohoué, Karthikeyan Bhargavan, Jonathan Protzenko, Benjamin Beurdouche
Jasmin: High-Assurance and High-Speed Cryptography [PDF] [Artifact] (H4)	José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Arthur Blot, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Hugo Pacheco, Benedikt Schmidt, Pierre-Yves Strub
Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives [PDF] (I1)	Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Greg Zaverucha
To BLISS-B or not to be - Attacking strongSwan's Implementation of Post-Quantum Signatures [PDF] [Paper] (I1)	Peter Pessl, Leon Groot Bruinderink, Yuval Yarom
Side-Channel Attacks on BLISS Lattice-Based Signatures: Exploiting Branch Tracing Against strongSwan and Electromagnetic Emanations in Microcontrollers [PDF] [Paper] [Artifact] (I1)	Thomas Espitau, Pierre-Alain Fouque, Benoït Gérard, Mehdi Tibouchi
Nonmalleable Information Flow Control [PDF] [Paper] (I2) ★	Ethan Cecchetti, Andrew Myers, Owen Arden
Cryptographically Secure Information Flow Control on Key-Value Stores [PDF] [Paper] (I2)	Lucas Waye, Pablo Buiras, Owen Arden, Alejandro Russo, Stephen Chong
Object Flow Integrity [PDF] (I2)	Wenhao Wang, Xiaoyang Xu, Kevin Hamlen

BBA+: Improving the Security and Applicability of Privacy-Preserving Point Collection [PDF] (I3)	Gunnar Hartung, Max Hoffmann, Matthias Nagel, Andy Rupp
walk2friends: Inferring Social Links from Mobility Profiles [PDF] [Paper] [Artifact] (I3)	Michael Backes, Mathias Humbert, Jun Pang, Yang Zhang
Back to the drawing board: Revisiting the design of optimal location privacy-preserving mechanisms [PDF] [Paper] (I3)	Simon Oya, Carmela Troncoso, Fernando Pérez-González
Certified Verification of Algebraic Properties on Low-Level Mathematical Constructs in Cryptographic Programs [PDF] (I4)	Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang
A Fast and Verified Software Stack for Secure Function Evaluation [PDF] [Paper] [Artifact] (I4)	José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte, Vitor Pereira
Verified Correctness and Security of mbedTLS HMAC-DRBG [PDF] [Paper] [Artifact] (I4)	Katherine Q. Ye, Matthew Green, Naphat Sanguansin, Lennart Beringer, Adam Petcher, Andrew W. Appel
How Unique is Your .onion? An Analysis of the Fingerprintability of Tor Onion Services [PDF] [Paper] [Artifact] (I5) ★	Rebekah Overdorf, Marc Juarez, Gunes Acar, Rachel Greenstadt, Claudia Diaz
The Waterfall of Liberty: Decoy Routing Circumvention that Resists Routing Attacks [PDF] [Artifact] (I5)	Milad Nasr, Hadi Zolfaghari, Amir Houmansadr
Compressive Traffic Analysis: A New Paradigm for Scalable Traffic Analysis [PDF] [Paper] (I5)	Milad Nasr, Amir Houmansadr, Arya Mazumdar
Full accounting for verifiable outsourcing [PDF] [Paper] (J1)	Riad S. Wahby, Ye Ji, Andrew J. Blumberg, abhi shelat, Justin Thaler, Michael Walfish, Thomas Wies

Ligero: Lightweight Sublinear Arguments Without a Trusted Setup [PDF] (J1)	Scott Ames, Carmit Hazay, Yuval Ishai, Muthuramakrishnan Venkitasubramaniam
Homomorphic Secret Sharing: Optimizations and Applications [PDF] [Artifact] (J1)	Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Michele Orru
DIFUZE: Interface Aware Fuzzing for Kernel Drivers [PDF] [Artifact] (J2)	Jake Corina, Aravind Machiry, Christopher Salls, Yan Shoshitaishvili, Shuang Hao, Christopher Kruegel, Giovanni Vigna
SemFuzz: Semantics-based Automatic Generation of Proof-of-Concept Exploits [PDF] (J2)	Wei You, Peiyuan Zong, Kai Chen, XiaoFeng Wang, Xiaojing Liao, Pan Bian, Bin Liang
SlowFuzz: Automated Domain-Independent Detection of Algorithmic Complexity Vulnerabilities [PDF] [Paper] (J2)	Theofilos Petsios, Jason Zhao, Angelos D. Keromytis, Suman Jana
Checking Open-Source License Violation and 1-day Security Risk at Large Scale [PDF] (J3)	Ruian Duan, Ashish Bijlani, Meng Xu, Taesoo Kim, Wenke Lee
Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android [PDF] [Paper] [Artifact] (J3)	Erik Derr, Sven Bugiel, Sascha Fahl, Yasemin Acar, Michael Backes
A Large-Scale Empirical Study of Security Patches [PDF] (J3)	Frank Li, Vern Paxson
DEFTL: Implementing Plausibly Deniable Encryption in Flash Translation Layer [PDF] (J4)	Shijie Jia, Luning Xia, Bo Chen, Peng Liu
FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware [PDF] (J4)	Jian Huang, Jun Xu, Xinyu Xing, Peng Liu, Moinuddin K. Qureshi
FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution [PDF] [Paper] (J4)	Grant Hernandez, Farhaan Fowze, Dave (Jing) Tian, Tuba Yavuz, Kevin Butler

TinyOLE: Efficient Actively Secure Two-Party Computation from Oblivious Linear Function Evaluation [PDF] (K1)	Nico Döttling, Satrajit Ghosh, Jesper Buus Nielsen, Tobias Nilges, Roberto Trifiletti
Distributed Measurement with Private Set-Union Cardinality [PDF] (K1)	Ellis Fenske, Akshaya Mani, Aaron Johnson, Micah Sherr
Efficient Public Trace-and-Revoke from Standard Assumptions [PDF] [Paper] (K1)	Shweta Agrawal, Sanjay Bhattacherjee, Duong Hieu Phan, Damien Stehle, Shota Yamada
Designing New Operating Primitives to Improve Fuzzing Performance [PDF] (K2)	Wen Xu, Sanidhya Kashyap, Changwoo Min, Taesoo Kim
Directed Greybox Fuzzing [PDF] [Paper] [Artifact] (K2)	Marcel Böhme, Van-Thuan Pham, Manh-Dung Nguyen, Abhik Roychoudhury
IMF: Inferred Model-based Fuzzer [PDF] [Artifact] (K2)	HyungSeok Han, Sang Kil Cha
PtrSplit: Supporting general pointers in automatic program partitioning [PDF] (K3)	Shen Liu, Gang Tan, Trent Jaeger
HexType: Efficient Detection of Type Confusion Errors for C++ [PDF] (K3)	Yuseok Jeon, Priyam Biswas, Scott Carr, Byoungyoung Lee, Mathias Payer
FreeGuard: A Faster Secure Heap Allocator [PDF] [Artifact] (K3)	Sam Silvestro, Hongyu Liu, Corey Crosser, Zhiqiang Lin, Tongping Liu
JITGuard: Hardening Just-in-time Compilers with SGX [PDF] [Paper] (K4)	Tommaso Frassetto, David Gens, Christopher Liebchen, Ahmad-Reza Sadeghi
Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX [PDF] (K4)	Wenhao Wang, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, XiaoFeng Wang, Vincent Bindschaedler, Haixu Tang, Carl A. Gunter

A Formal Foundation for Secure Remote Execution of Enclaves [PDF] [Paper] [Artifact] (K4) ★	Pramod Subramanyan, Rohit Sinha, Ilia Lebedev, Srinivas Devadas, Sanjit Seshia