Message from the General Chair

Organizing Committee

Program Committee

External Reviewers

Hardware-Aided Security

- Protecting Private Keys against Memory Disclosure Attacks Using Hardware
  Transactional Memory
  Le Guan, Jingqiang Lin, Bo Luo, Jiwu Jing, and Jing Wang

- CHERI: A Hybrid Capability-System Architecture for Scalable Software
  Compartamentalization
  Robert N.M. Watson, Jonathan Woodruff, Peter G. Neumann, Simon W. Moore,
  Jonathan Anderson, David Chisnall, Nirav Dave, Brooks Davis, Khilan Gudka,
  Ben Laurie, Steven J. Murdoch, Robert Norton, Michael Roe, Stacey Son,
  and Munraj Vadera

- VC3: Trustworthy Data Analytics in the Cloud Using SGX
  Felix Schuster, Manuel Costa, Cédric Fournet, Christos Gkantsidis,
  Marcus Peinado, Gloria Mainar-Ruiz, and Mark Russinovich

- Using Hardware Features for Increased Debugging Transparency
  Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun

- Virtual Proofs of Reality and their Physical Implementation
  Ulrich Rührmair, J.L. Martinez-Hurtado, Xiaolin Xu, Christian Kraeh,
  Christian Hilgers, Dima Kononchuk, Jonathan J. Finley, and Wayne P. Burleson

Cryptocurrencies and Cybercrime

- The Miner's Dilemma
  Ittay Eyal
SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies ..................................................104
Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan,
Joshua A. Kroll, and Edward W. Felten

Bitcoin over Tor isn’t a Good Idea ..........................................................................................................................122
Alex Biryukov and Ivan Pustogarov

Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting ..........................................................135
Mohammad Taha Khan, Xiang Huo, Zhou Li, and Chris Kanich

Ad Injection at Scale: Assessing Deceptive Advertisement Modifications ............................................................151
Kurt Thomas, Elie Bursztein, Chris Grier, Grant Ho, Nav Jagpal,
Alexandros Kapravelos, Damon Mccoy, Antonio Nappa, Vern Paxson,
Paul Pearce, Niels Provos, and Moheeb Abu Rajab

Protocols and Network Security
Connection-Oriented DNS to Improve Privacy and Security ......................................................................................171
Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin,
and Nikita Somaiya

Temporal Lensing and Its Application in Pulsing Denial-of-Service Attacks ............................................................187
Ryan Rasti, Mukul Murthy, Nicholas Weaver, and Vern Paxson

Secure Track Verification ..................................................................................................................................199
Matthias Schäfer, Vincent Lenders, and Jens Schmitt

How Secure and Quick is QUIC? Provable Security and Performance Analyses ......................................................214
Robert Lychev, Samuel Jero, Alexandra Boldyreva, and Cristina Nita-Rotaru

SoK: Secure Messaging .....................................................................................................................................232
Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl,
Ian Goldberg, and Matthew Smith

Cryptographic Protocols
Geppetto: Versatile Verifiable Computation .................................................................................................................253
Craig Costello, Cédric Fournet, Jon Howell, Markulf Kohlweiss,
Benjamin Kreuter, Michael Naehrig, Bryan Parno, and Samee Zahur

ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data ......................................................271
Michael Backes, Manuel Barbosa, Dario Fiore, and Raphael M. Reischuk

Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs ..........................................................287
Eli Ben-Sasson, Alessandro Chiesa, Matthew Green, Eran Tromer,
and Madars Virza
Forward Secure Asynchronous Messaging from Puncturable Encryption .................................305
Matthew D. Green and Ian Miers

Riposte: An Anonymous Messaging System Handling Millions of Users ...............................321
Henry Corrigan-Gibbs, Dan Boneh, and David Mazières

ORAM and Secure Multi-party Computation
Privacy and Access Control for Outsourced Personal Records ...........................................341
Matteo Maffei, Giulio Malavolta, Manuel Reinert, and Dominique Schröder

OblIVM: A Programming Framework for Secure Computation .........................................359
Chang Liu, Xiao Shaun Wang, Kartik Nayak, Yan Huang, and Elaine Shi

GraphSC: Parallel Secure Computation Made Easy ..........................................................377
Kartik Nayak, Xiao Shaun Wang, Stratis Ioannidis, Udi Weinsberg, Nina Taft, and Elaine Shi

Malicious-Client Security in Blind Seer: A Scalable Private DBMS ..................................395
Ben A. Fisc, Binh Vo, Fernando Krell, Abishek Kumarasubramanian, Vladimir Kolesnikov, Tal Malkin, and Steven M. Bellovin

TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits .......................411
Ebrahim M. Songhori, Siam U. Hussain, Ahmad-Reza Sadeghi, Thomas Schneider, and Farinaz Koushanfar

Security du Jour
SurroundWeb: Mitigating Privacy Concerns in a 3D Web Browser ....................................431
John Vilk, David Molnar, Benjamin Livshits, Eyal Ofek, Chris Rossbach, Alexander Moshchuk, Helen J. Wang, and Ran Gal

GenoGuard: Protecting Genomic Data against Brute-Force Attacks ..................................447
Zhicong Huang, Erman Ayday, Jacques Fellay, Jean-Pierre Hubaux, and Ari Juels

Towards Making Systems Forget with Machine Unlearning ..............................................463
Yinzhi Cao and Junfeng Yang

Cracking-Resistant Password Vaults Using Natural Language Encoders ..........................481
Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart

SoK: A Comprehensive Analysis of Game-Based Ballot Privacy Definitions .......................499
David Bernhard, Véronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi
Protocols

Vetting SSL Usage in Applications with SSLINT .......................................................................................519
  Boyuan He, Vaibhav Rastogi, Yinzhi Cao, Yan Chen, V.N. Venkatakrishnan, Runqing Yang, and Zhenrui Zhang

A Messy State of the Union: Taming the Composite State Machines of TLS ........................................535
  Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Jean Karim Zinzindohoue

Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem ..........................................................553
  Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila

Security of the J-PAKE Password-Authenticated Key Exchange Protocol ........................................571
  Michel Abdalla, Fabrice Benhamouda, and Philip MacKenzie

Side Channels

S$A: A Shared Cache Attack That Works across Cores and Defies VM Sandboxing—and Its Application to AES ........................................................................................................605
  Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar

Last-Level Cache Side-Channel Attacks are Practical .............................................................................623
  Fangfei Liu, Yuval Yarom, Qian Ge, Gernot Heiser, and Ruby B. Lee

On Subnormal Floating Point and Abnormal Timing ..............................................................................640
  Marc Andrysco, David Kohlbrenner, Keaton Mowery, Ranjit Jhala, Sorin Lerner, and Hovav Shacham

Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems .....................659
  Yuanzhong Xu, Weidong Cui, and Marcus Peinado

Malware and Program Analysis

SoK: Deep Packer Inspection: A Longitudinal Study of the Complexity of Run-Time Packers ..................674
  Xabier Ugarte-Pedrero, Davide Balzarotti, Igor Santos, and Pablo G. Bringas

A Generic Approach to Automatic Deobfuscation of Executable Code ..................................................692
  Babak Yadegari, Brian Johannesmeyer, Ben Whitely, and Saumya Debray

  Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero, and Tudor Dumitraș
Cross-Architecture Bug Search in Binary Executables ................................................................. 709
  Jannik Pewny, Behrad Garmany, Robert Gawlik, Christian Rossow,
  and Thorsten Holz

Program-Adaptive Mutational Fuzzing ........................................................................................... 725
  Sang Kil Cha, Maverick Woo, and David Brumley

**Memory Integrity**

Counterfeit Object-oriented Programming: On the Difficulty of Preventing Code Reuse Attacks in C++ Applications .............................................................................................................. 745
  Felix Schuster, Thomas Tendyck, Christopher Liebchen, Lucas Davi,
  Ahmad-Reza Sadeghi, and Thorsten Holz

Readactor: Practical Code Randomization Resilient to Memory Disclosure ........................................ 763
  Stephen Crane, Christopher Liebchen, Andrei Homescu, Lucas Davi,
  Per Larsen, Ahmad-Reza Sadeghi, Stefan Brunthaler, and Michael Franz

Missing the Point(er): On the Effectiveness of Code Pointer Integrity .............................................. 781
  Isaac Evans, Sam Fingeret, Julian Gonzalez, Ulziibayar Otgonbaatar,
  Tiffany Tang, Howard Shrobe, Stelios Sidiropoulos-Douskos, Martin Rinard,
  and Hamed Okhravi

Automatic Inference of Search Patterns for Taint-Style Vulnerabilities ........................................... 797
  Fabian Yamaguchi, Alwin Maier, Hugo Gascon, and Konrad Rieck

Micro-Policies: Formally Verified, Tag-Based Security Monitors ..................................................... 813
  Arthur Azevedo de Amorim, Maxime Dénès, Nick Giannarakis, Cătălin Hriţcu,
  Benjamin C. Pierce, Antal Spector-Zabusky, and Andrew Tolmach

**Security du Jour II**

Securing Multiparty Online Services Via Certification of Symbolic Transactions .................................. 833
  Eric Y. Chen, Shuo Chen, Shaz Qadeer, and Rui Wang

Understanding and Monitoring Embedded Web Scripts ...................................................................... 850
  Yuchen Zhou and David Evans

High System-Code Security with Low Overhead .................................................................................. 866
  Jonas Wagner, Volodymyr Kuznetsov, George Candea, and Johannes Kinder

Caelus: Verifying the Consistency of Cloud Services with Battery-Powered Devices ................................ 880
  Beom Heyn Kim and David Lie
Android Security

Effective Real-Time Android Application Auditing .................................................................899
  Mingyuan Xia, Lu Gong, Yuanhao Lyu, Zhengwei Qi, and Xue Liu

Leave Me Alone: App-Level Protection against Runtime Information Gathering
on Android ......................................................................................................................................915
  Nan Zhang, Kan Yuan, Muhammad Naveed, Xiaoyong Zhou, and Xiaofeng Wang

What the App is That? Deception and Countermeasures in the Android User
Interface ....................................................................................................................................931
  Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio,
  Christopher Kruegel, and Giovanni Vigna

Author Index ................................................................................................................................949