Session 1: Programming Language Security

All Your IFCException Are Belong to Us ................................................................. 3
    Catalin Hritcu, Michael Greenberg, Ben Karel, Benjamin C. Pierce, and Greg Morrisett

Declarative, Temporal, and Practical Programming with Capabilities .................................. 18
    William R. Harris, Somesh Jha, Thomas Reps, Jonathan Anderson, and Robert N.M. Watson

Towards Practical Reactive Security Audit Using Extended Static Checkers .......................... 33
    Julien Vanegue and Shuvendu K. Lahiri

SoK: Eternal War in Memory ......................................................................................... 48
    László Szekeres, Mathias Payer, Tao Wei, and Dawn Song

Session 2: Anonymous Network Communication

The Parrot Is Dead: Observing Unobservable Network Communications ............................... 65
    Amir Houmansadr, Chad Brubaker, and Vitaly Shmatikov

Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization ...................... 80
    Alex Biryukov, Ivan Pustogarov, and Raif-Philipp Weinmann

Session 3: Botnets and Other Underground Activities

SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets ................. 97
    Christian Rossow, Dennis Andriesse, Tillmann Werner, Brett Stone-Gross,
    Daniel Plöhmann, Christian J. Dietrich, and Herbert Bos

Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts
    on Malicious Web Infrastructures ........................................................................ 112
    Zhou Li, Sumayah Alrwais, Yinglian Xie, Fang Yu, and XiaoFeng Wang

The Crossfire Attack ................................................................................................. 127
    Min Suk Kang, Soo Bum Lee, and Virgil D. Gligor
Session 4: Jamming Uses and Defenses

Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors .................................................. 145
  Denis Foo Kune, John Backes, Shane S. Clark, Daniel Kramer, Matthew Reynolds,
  Kevin Fu, Yongdae Kim, and Wenyuan Xu

On Limitations of Friendly Jamming for Confidentiality................................................................. 160
  Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan, and Srdjan Capkun

Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time .................................................. 174
  Wenbo Shen, Peng Ning, Xiaofan He, and Huaiyu Dai

Session 5: Secure Operating Systems I

Practical Timing Side Channel Attacks against Kernel Space ASLR .................................................. 191
  Ralf Hund, Carsten Willems, and Thorsten Holz

PrivExec: Private Execution as an Operating System Service .................................................. 206
  Kaan Onarlioglu, Collin Mulliner, William Robertson, and Engin Kirda

Session 6: Cryptographic Tools for Building Verifiable Cloud Computing

A Hybrid Architecture for Interactive Verifiable Computation .................................................. 223
  Victor Vu, Srinath Setty, Andrew J. Blumberg, and Michael Walfish

Pinocchio: Nearly Practical Verifiable Computation .................................................. 238
  Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova

ObliviStore: High Performance Oblivious Cloud Storage .................................................. 253
  Emil Stefanov and Elaine Shi

Session 7: Hardware Security

Hiding Information in Flash Memory .................................................. 271
  Yinglei Wang, Wing-kei Yu, Sarah Q. Xu, Edwin Kan, and G. Edward Suh

PUFs in Security Protocols: Attack Models and Security Evaluations .................................................. 286
  Ulrich Rührmair and Marten van Dijk

SoK: Secure Data Deletion .................................................. 301
  Joel Reardon, David Basin, and Srdjan Capkun
Session 8: Privacy

Anon-Pass: Practical Anonymous Subscriptions ................................................................. 319
  Michael Z. Lee, Alan M. Dunn, Brent Waters, Emmett Witchel, and Jonathan Katz

Privacy-Preserving Ridge Regression on Hundreds of Millions of Records ......................... 334
  Valeria Nikolaenko, Udi Weinsberg, Stratis Ioannidis, Marc Joye, Dan Boneh,
  and Nina Taft

A Scanner Darkly: Protecting User Privacy from Perceptual Applications ........................ 349
  Suman Jana, Arvind Narayanan, and Vitaly Shmatikov

Session 9: Application Security

Caveat Coercitor: Coercion-Evidence in Electronic Voting .............................................. 367
  Gurchetan S. Grewal, Mark D. Ryan, Sergiu Bursuc, and Peter Y.A. Ryan

SoK: The Evolution of Sybil Defense via Social Networks .............................................. 382
  Lorenzo Alvisi, Allen Clement, Alessandro Epasto, Silvio Lattanzi, and Alessandro Panconesi

Zerocoin: Anonymous Distributed E-Cash from Bitcoin ............................................... 397
  Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin

Session 10: Formal Methods for Building Secure Systems

seL4: From General Purpose to a Proof of Information Flow Enforcement .................... 415
  Toby Murray, Daniel Matichuk, Matthew Brassil, Peter Gammie, Timothy Bourke,
  Sean Seefried, Corey Lewis, Xin Gao, and Gerwin Klein

Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework 430
  Amit Vasudevan, Sagar Chaki, Limin Jia, Jonathan McCune, James Newsome,
  and Anupam Datta

Implementing TLS with Verified Cryptographic Security ............................................. 445
  Karthikeyan Bhargavan, Cédric Fouquet, Markulf Kohlweiss, Alfredo Pironti,
  and Pierre-Yves Strub

Session 11: Crypto

An Ideal-Security Protocol for Order-Preserving Encoding ........................................... 463
  Raluca Ada Popa, Frank H. Li, and Nickolai Zeldovich

Efficient Garbling from a Fixed-Key Blockcipher .................................................... 478
  Mihir Bellare, Viet Tung Hoang, Sriram Keelvedhi, and Phillip Rogaway

Circuit Structures for Improving Efficiency of Security and Privacy Tools .................... 493
  Samee Zahur and David Evans
Session 12: SSL/TLS and Web Security

SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements ................................................................. 511
Jeremy Clark and Paul C. van Oorschot

Lucky Thirteen: Breaking the TLS and DTLS Record Protocols ......................................................... 526
Nadhem J. AlFardan and Kenneth G. Paterson

Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting.......................... 541
Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel,
Frank Piessens, and Giovanni Vigna

Session 13: Secure Operating Systems II

Practical Control Flow Integrity and Randomization for Binary Executables ........................................ 559
Chao Zhang, Tao Wei, Zhaofeng Chen, Lei Duan, László Szekeres, Stephen McCamant,
Dawn Song, and Wei Zou

Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization ........................................................................ 574
Kevin Z. Snow, Fabian Monrose, Lucas Davi, Alexandra Dmitrienko,
Christopher Liebchen, and Ahmad-Reza Sadeghi

Welcome to the Entropies: Boot-Time Entropy in Embedded Devices ................................................... 589
Keaton Mowery, Michael Wei, David Kohlbrenner, Hovav Shacham, and Steven Swanson

Author Index ........................................................................................................................................ 605