IEEE Symposium on Security and Privacy 2013 • Program At-A-Glance

MONDAY, 20 MAY 2013

7:30 – 8:30am **Registration and Breakfast**
Registration Location: Italian Foyer

8:30 – 8:45am **Opening Remarks**

8:45 – 10:25am **Session 1: Programming Language Security**
Session Chair: Ben Livshits

All Your IFCException Are Belong To Us *by C. Hritcu, M. Greenberg, B. Karel, B. C. Pierce, G. Morrisett*

Declarative, Temporal, and Practical Programming with Capabilities *by W. R. Harris, S. Jha, T. Reps, J. Anderson, R. N. M. Watson*

Towards Practical Reactive Security Audit Using Extended Static Checkers *by J. Vanegue, S. K. Lahiri*

SoK: Eternal War in Memory *by L. Szekeres, M. Payer, T. Wei, D. Song*

10:25 – 10:55am **Break**

10:55 – 11:45am **Session 2: Anonymous Network Communication**
Session Chair: Srdjan Capkun

The Parrot is Dead: Observing Unobservable Network Communications *by A. Houmansadr, C. Brubaker, V. Shmatikov*

Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization *by A. Biryukov, I. Pustogarov, R. Weinmann*

11:45 – 1:00pm **Lunch**

1:00 – 2:15pm **Session 3: Botnets and Other Underground Activities**
Session Chair: Thorsten Holz

SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets *by C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, H. Bos*

Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures *by Z. Li, S. Alrwais, Y. Xie, F. Yu, and X. Wang*

The Crossfire Attack *by M. S. Kang, S. B. Lee, and V. D. Gligor*

2:15 – 2:45pm **Break**

2:45 – 4:00pm **Session 4: Jamming Uses and Defenses**
Session Chair: Yinglian Xie

Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors *by D. F. Kune, J. Backes, S. Clark, D. Kramer MD, M. Reynolds MD, K. Fu, Y. Kim, W. Xu*

On Limitations of Friendly Jamming for Confidentiality *By N. Ole Tippenhauer, L. Malisa, A. Ranganathan, S. Capkun*

Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time *by W. Shen, P. Ning, X. He, H. Dai*

4:00 – 4:30pm **Break**

4:30 – 5:25pm **Session 5: Secure Operating Systems (I)**
Session Chair: Ahmad-Reza Sadeghi

Practical Timing Side Channel Attacks Against Kernel Space ASLR *by R. Hund, C. Willems, T. Holz*

PrivExec: Private Execution as an Operating System Service *by K. Onarlioglu, C. Mulliner, W. Robertson, E. Kirda*

6:00 – 8:00pm **Poster Session and Reception**
Location: California Room

TUESDAY, 21 MAY 2013

7:30 – 8:30am **Breakfast**

8:30 – 8:45am **Awards**

8:45 – 10:00am **Session 6: Cryptographic Tools for Building Verifiable Cloud Computing**
Session Chair: XiaoFeng Wang

A Hybrid Architecture for Interactive Verifiable Computation *by V. Vu, S. Setty, A. J. Blumberg, M. Walfish*

Pinocchio: Nearly Practical Verifiable Computation *by B. Parno, C. Gentry, J. Howell, M. Raykova*

ObliviStore: High Performance Oblivious Cloud Storage *by E. Stefanov, E. Shi*

10:00 – 10:30am **Break**

10:30 – 11:45am **Session 7: Hardware Security**
Session Chair: Jon McCune

Hiding Information in Flash Memory *by Y. Wang, W. Yu, S. Q. Xu, E. Kan, G. E. Suh*

PUFs in Security Protocols: Attack Models and Security Evaluations *by U. Rührmair, M. van Dijk*

SoK: Secure Data Deletion *by J. Reardon, D. Basin, S. Capkun*

11:45 – 1:00pm **Lunch**

1:00 – 2:15pm **Session 8: Privacy**
Session Chair: Anupam Datta

Anon-Pass: Practical Anonymous Subscriptions *by M. Z. Lee, A. M. Dunn, B. Waters, E. Witchel, J. Katz*

Privacy-Preserving Ridge Regression on Hundreds of Millions of Records *by V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, N. Taft*

A Scanner Darkly: Protecting User Privacy From Perceptual Applications *by S. Jana, A. Narayanan, V. Shmatikov*

2:15 – 2:45pm **Break**

2:45 – 4:00pm **Session 9: Application Security (Voting, Sybil, Bitcoin)**
Session Chair: Matteo Maffei

Caveat Coercitor: Coercion-Evidence in Electronic Voting *by G. S. Grewal, M. D. Ryan, S. Bursuc, P. Y. A. Ryan*

SoK: The Evolution of Sybil Defense via Social Networks *by L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, A. Panconesi*

Zerocoin: Anonymous Distributed E-Cash from Bitcoin *by I. Miers, C. Garman, M. Green, A. D. Rubin*

4:00 – 4:30pm **Break**

4:30 – 5:45pm **Short Talks**

6:00 – 7:00pm **Business Meeting**
Location: Grand Ballroom

WEDNESDAY, 22 MAY 2013

7:30 – 8:30am **Breakfast**

8:30 – 8:45am **Remarks**

8:45 – 10:00am **Session 10: Formal Methods**
Session Chair: Lujo Bauer

seL4: from General Purpose to a Proof of Information Flow Enforcement *by T. Murray, D. Matichuk, M. Brassil, P. Gammie, T. Bourke, S. Seefried, C. Lewis, X. Gao, G. Klein*

Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework *by A. Vasudevan, S. Chaki, L. Jia, J. M. McCune, J. Newsome, A. Datta*

Implementing TLS with Verified Cryptographic Security *by K. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, P. Strub*

10:00 – 10:30am **Break**

10:30 – 11:45am **Session 11: Crypto**
Session Chair: Bryan Parno

An Ideal-Security Protocol for Order-Preserving Encoding *by R. A. Popa, F. Li, N. Zeldovich*

Efficient Garbling from a FixedKey Blockcipher *by M. Bellare, V. T. Hoang, S. Keelveedhi, P. Rogaway*

Circuit Structures for Improving Efficiency of Security and Privacy Tools *by S. Zahur, D. Evans*

11:45 – 1:00pm **Lunch**

1:00 – 2:15pm **Session 12: SSL / TLS, Web Security**
Session Chair: Kapil Singh

SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements *by J. Clark, P. van Oorschot*

Lucky Thirteen: Breaking the TLS and DTLS Record Protocols *by N. J. AlFardan, K. G. Paterson*

Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting *by N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, G. Vigna*

2:15 – 2:45pm **Break**

2:45 – 4:00pm **Session 13: Secure Operating Systems (II)**
Session Chair: Herbert Bos

Practical Control Flow Integrity & Randomization for Binary Executables *by C. Zhang, T. Wei, Z. Chen, L. Duan, L. Szekeres, S. McCamant, D. Song, W. Zou*

Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization *by K. Z. Snow, F. Monrose, L. Davi, A. Dmitrienko, C. Liebchen, A. Sadeghi*

Welcome to the Entropics: Boot-Time Entropy in Embedded Devices *by K. Mowery, M. Wei, D. Kohlbrenner, H. Shacham, S. Swanson*

4:00 – 4:30pm **Break**

4:30 – 5:45pm **Panel Discussion: Privacy Research**
Moderator: Daniel Weitzner, MIT

Vijay Atluri, *NSF* • Joan Feigenbaum, *Yale* • Karyn Higa-Smith, *DHS* • Deirdre Mulligan, *UCB* • Betsy Masiello, *Google* • Jeannette Wing, *MRI*

6:00 – 7:30pm **S&P / SPW Bridging Reception**
Location: California Room WEST

6:30 – 7:30pm **Birds-of-a-Feather Sessions**
Location: Elizabethan Rooms