

# **2013 IEEE Symposium on Security and Privacy**

**(SP 2013)**

**Berkeley, California, USA  
19 – 22 May 2013**



**IEEE Catalog Number: CFP13020-RQF**  
**ISBN: 978-1-4673-6166-8**

# 2013 IEEE Symposium on Security and Privacy SP 2013

Message from the General Chair.....	ix
Message from the Program Committee Chairs.....	xi
Organizing Committee.....	xii
Program Committee.....	xiii
External Reviewers .....	xv

## Session 1: Programming Language Security

All Your IFCEException Are Belong to Us.....	3
<i>Catalin Hritcu, Michael Greenberg, Ben Karel, Benjamin C. Pierce, and Greg Morrisett</i>	
Declarative, Temporal, and Practical Programming with Capabilities.....	18
<i>William R. Harris, Somesh Jha, Thomas Reps, Jonathan Anderson, and Robert N.M. Watson</i>	
Towards Practical Reactive Security Audit Using Extended Static Checkers .....	33
<i>Julien Vanegue and Shuvendu K. Lahiri</i>	
SoK: Eternal War in Memory.....	48
<i>László Szekeres, Mathias Payer, Tao Wei, and Dawn Song</i>	

## Session 2: Anonymous Network Communication

The Parrot Is Dead: Observing Unobservable Network Communications.....	65
<i>Amir Houmansadr, Chad Brubaker, and Vitaly Shmatikov</i>	
Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization .....	80
<i>Alex Biryukov, Ivan Pustogarov, and Ralf-Philipp Weinmann</i>	

## Session 3: Botnets and Other Underground Activities

SoK: P2PWNET - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets.....	97
<i>Christian Rossow, Dennis Andriess, Tillmann Werner, Brett Stone-Gross, Daniel Plohmann, Christian J. Dietrich, and Herbert Bos</i>	
Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures.....	112
<i>Zhou Li, Sumayah Alrwais, Yinglian Xie, Fang Yu, and XiaoFeng Wang</i>	
The Crossfire Attack.....	127
<i>Min Suk Kang, Soo Bum Lee, and Virgil D. Gligor</i>	

## **Session 4: Jamming Uses and Defenses**

Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors .....	145
<i>Denis Foo Kune, John Backes, Shane S. Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyan Xu</i>	
On Limitations of Friendly Jamming for Confidentiality.....	160
<i>Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan, and Srdjan Capkun</i>	
Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time .....	174
<i>Wenbo Shen, Peng Ning, Xiaofan He, and Huaiyu Dai</i>	

## **Session 5: Secure Operating Systems I**

Practical Timing Side Channel Attacks against Kernel Space ASLR .....	191
<i>Ralf Hund, Carsten Willems, and Thorsten Holz</i>	
PrivExec: Private Execution as an Operating System Service.....	206
<i>Kaan Onarlioglu, Collin Mulliner, William Robertson, and Engin Kirda</i>	

## **Session 6: Cryptographic Tools for Building Verifiable Cloud Computing**

A Hybrid Architecture for Interactive Verifiable Computation.....	223
<i>Victor Vu, Srinath Setty, Andrew J. Blumberg, and Michael Walfish</i>	
Pinocchio: Nearly Practical Verifiable Computation.....	238
<i>Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova</i>	
ObliviStore: High Performance Oblivious Cloud Storage .....	253
<i>Emil Stefanov and Elaine Shi</i>	

## **Session 7: Hardware Security**

Hiding Information in Flash Memory .....	271
<i>Yinglei Wang, Wing-kei Yu, Sarah Q. Xu, Edwin Kan, and G. Edward Suh</i>	
PUFs in Security Protocols: Attack Models and Security Evaluations.....	286
<i>Ulrich Rührmair and Marten van Dijk</i>	
SoK: Secure Data Deletion .....	301
<i>Joel Reardon, David Basin, and Srdjan Capkun</i>	

## Session 8: Privacy

Anon-Pass: Practical Anonymous Subscriptions .....	319
<i>Michael Z. Lee, Alan M. Dunn, Brent Waters, Emmett Witchel, and Jonathan Katz</i>	
Privacy-Preserving Ridge Regression on Hundreds of Millions of Records .....	334
<i>Valeria Nikolaenko, Udi Weinsberg, Stratis Ioannidis, Marc Joye, Dan Boneh, and Nina Taft</i>	
A Scanner Darkly: Protecting User Privacy from Perceptual Applications .....	349
<i>Suman Jana, Arvind Narayanan, and Vitaly Shmatikov</i>	

## Session 9: Application Security

Caveat Coercitor: Coercion-Evidence in Electronic Voting .....	367
<i>Gurchetan S. Grewal, Mark D. Ryan, Sergiu Bursuc, and Peter Y.A. Ryan</i>	
SoK: The Evolution of Sybil Defense via Social Networks .....	382
<i>Lorenzo Alvisi, Allen Clement, Alessandro Epasto, Silvio Lattanzi, and Alessandro Panconesi</i>	
ZeroCoin: Anonymous Distributed E-Cash from Bitcoin .....	397
<i>Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin</i>	

## Session 10: Formal Methods for Building Secure Systems

sel4: From General Purpose to a Proof of Information Flow Enforcement .....	415
<i>Toby Murray, Daniel Matichuk, Matthew Brassil, Peter Gammie, Timothy Bourke, Sean Seefried, Corey Lewis, Xin Gao, and Gerwin Klein</i>	
Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework .....	430
<i>Amit Vasudevan, Sagar Chaki, Limin Jia, Jonathan McCune, James Newsome, and Anupam Datta</i>	
Implementing TLS with Verified Cryptographic Security .....	445
<i>Karthikeyan Bhargavan, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, and Pierre-Yves Strub</i>	

## Session 11: Crypto

An Ideal-Security Protocol for Order-Preserving Encoding .....	463
<i>Raluca Ada Popa, Frank H. Li, and Nikolai Zeldovich</i>	
Efficient Garbling from a Fixed-Key Blockcipher .....	478
<i>Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway</i>	
Circuit Structures for Improving Efficiency of Security and Privacy Tools .....	493
<i>Samee Zahur and David Evans</i>	

## Session 12: SSL/TLS and Web Security

SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements .....	511
<i>Jeremy Clark and Paul C. van Oorschot</i>	
Lucky Thirteen: Breaking the TLS and DTLS Record Protocols.....	526
<i>Nadhem J. Al Fardan and Kenneth G. Paterson</i>	
Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting.....	541
<i>Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna</i>	

## Session 13: Secure Operating Systems II

Practical Control Flow Integrity and Randomization for Binary Executables.....	559
<i>Chao Zhang, Tao Wei, Zhaofeng Chen, Lei Duan, László Szekeres, Stephen McCamant, Dawn Song, and Wei Zou</i>	
Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization .....	574
<i>Kevin Z. Snow, Fabian Monrose, Lucas Davi, Alexandra Dmitrienko, Christopher Liebchen, and Ahmad-Reza Sadeghi</i>	
Welcome to the Entropics: Boot-Time Entropy in Embedded Devices.....	589
<i>Keaton Mowery, Michael Wei, David Kohlbrenner, Hovav Shacham, and Steven Swanson</i>	
<b>Author Index .....</b>	<b>605</b>