

**22nd USENIX Security Symposium**  
**August 14–16, 2013**  
**Washington, D.C.**

Message from the Program Chair ..... vii

**Wednesday, August 14, 2013**

**Network Security**

**Greystar: Fast and Accurate Detection of SMS Spam Numbers in Large Cellular Networks using Grey Phone Space** .....1  
Nan Jiang, *University of Minnesota*; Yu Jin and Ann Skudlark, *AT&T Labs*; Zhi-Li Zhang, *University of Minnesota*

**Practical Comprehensive Bounds on Surreptitious Communication Over DNS** .....17  
Vern Paxson, *University of California, Berkeley, and International Computer Science Institute*; Mihai Christodorescu, *Qualcomm Research*; Mobin Javed, *University of California, Berkeley*; Josyula Rao, Reiner Sailer, Douglas Lee Schales, and Marc Ph. Stoecklin, *IBM Research*; Kurt Thomas, *University of California, Berkeley*; Wietse Venema, *IBM Research*; Nicholas Weaver, *ICSI and University of California, San Diego*

**Let Me Answer That For You: Exploiting Broadcast Information in Cellular Networks** .....33  
Nico Golde, Kévin Redon, and Jean-Pierre Seifert, *Deutsche Technische Universität Berlin and Telekom Innovation Laboratories*

**Potpourri**

**Dowsing for Overflows: A Guided Fuzzer to Find Buffer Boundary Violations** .....49  
Istvan Haller and Asia Slowinska, *VU University Amsterdam*; Matthias Neugschwandtner, *Vienna University of Technology*; Herbert Bos, *VU University Amsterdam*

**MetaSymplloit: Day-One Defense against Script-based Attacks with Security-Enhanced Symbolic Analysis** .....65  
Ruowen Wang, Peng Ning, Tao Xie, and Quan Chen, *North Carolina State University*

**Towards Automatic Software Lineage Inference** .....81  
Jiyong Jang, Maverick Woo, and David Brumley, *Carnegie Mellon University*

**Mobile Security I**

**Securing Embedded User Interfaces: Android and Beyond** .....97  
Franziska Roesner and Tadayoshi Kohno, *University of Washington*

**Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications** .....113  
Benjamin Livshits and Jaeyeon Jung, *Microsoft Research*

**Flexible and Fine-grained Mandatory Access Control on Android for Diverse Security and Privacy Policies** .....131  
Sven Bugiel, *Saarland University*; Stephan Heuser, *Fraunhofer SIT*; Ahmad-Reza Sadeghi, *Technische Universität Darmstadt and Center for Advanced Security Research Darmstadt*

(Wednesday, August 14, continues on p. iv)

## Applied Crypto I

**Proactively Accountable Anonymous Messaging in Verdict** .....147  
Henry Corrigan-Gibbs, David Isaac Wolinsky, and Bryan Ford, *Yale University*

**ZQL: A Compiler for Privacy-Preserving Data Processing** .....163  
Cédric Fournet, Markuld Kohlweiss, and George Danezis, *Microsoft Research*; Zhengqin Luo, *MSR-INRIA Joint Centre*

**DupLESS: Server-Aided Encryption for Deduplicated Storage** .....179  
Mihir Bellare and Sriram Keelveedhi, *University of California, San Diego*; Thomas Ristenpart, *University of Wisconsin-Madison*

## Large-Scale Systems Security I

**Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse** ....195  
Kurt Thomas, *University of California, Berkeley, and Twitter*; Damon McCoy, *George Mason University*; Chris Grier, *University of California, Berkeley, and International Computer Science Institute*; Alek Kolcz, *Twitter*; Vern Paxson, *University of California, Berkeley, and International Computer Science Institute*

**Impression Fraud in On-line Advertising via Pay-Per-View Networks**.....211  
Kevin Springborn, *Broadcast Interactive Media*; Paul Barford, *Broadcast Interactive Media and University of Wisconsin-Madison*

**The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions** .....227  
Tao Zhu, *Independent Researcher*; David Phipps, *Bowdoin College*; Adam Pridgen, *Rice University*; Jedidiah R. Crandall, *University of New Mexico*; Dan S. Wallach, *Rice University*

## Thursday, August 15, 2013

### Large-Scale Systems Security II

**You Are How You Click: Clickstream Analysis for Sybil Detection** .....241  
Gang Wang and Tristan Konolige, *University of California, Santa Barbara*; Christo Wilson, *Northeastern University*; Xiao Wang, *Renren Inc.*; Haitao Zheng and Ben Y. Zhao, *University of California, Santa Barbara*

**Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness** .....257  
Devdatta Akhawe, *University of California, Berkeley*; Adrienne Porter Felt, *Google, Inc.*

**An Empirical Study of Vulnerability Rewards Programs** .....273  
Matthew Finifter, Devdatta Akhawe, and David Wagner, *University of California, Berkeley*

### Applied Crypto II

**Secure Outsourced Garbled Circuit Evaluation for Mobile Devices** .....289  
Henry Carter, *Georgia Institute of Technology*; Benjamin Mood, *University of Oregon*; Patrick Traynor, *Georgia Institute of Technology*; Kevin Butler, *University of Oregon*

**On the Security of RC4 in TLS** .....305  
Nadhem AlFardan, *Royal Holloway, University of London*; Daniel J. Bernstein, *University of Illinois at Chicago and Technische Universiteit Eindhoven*; Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt, *Royal Holloway, University of London*

**PCF: A Portable Circuit Format for Scalable Two-Party Secure Computation** .....321  
Ben Kreuter, *University of Virginia*; Benjamin Mood, *University of Oregon*; abhi shelat, *University of Virginia*; Kevin Butler, *University of Oregon*

## Protecting and Understanding Binaries

**Control Flow Integrity for COTS Binaries** .....337  
Mingwei Zhang and R. Sekar, *Stony Brook University*

**Native x86 Decompilation Using Semantics-Preserving Structural Analysis and Iterative Control-Flow Structuring** .....353  
Edward J. Schwartz, *Carnegie Mellon University*; JongHyup Lee, *Korea National University of Transportation*; Maverick Woo and David Brumley, *Carnegie Mellon University*

**Strato: A Retargetable Framework for Low-Level Inlined-Reference Monitors** .....369  
Bin Zeng and Gang Tan, *Lehigh University*; Úlfar Erlingsson, *Google Inc.*

## Current and Future Systems Security

**On the Security of Picture Gesture Authentication** .....383  
Ziming Zhao and Gail-Joon Ahn, *Arizona State University and GFS Technology, Inc.*; Jeong-Jin Seo, *Arizona State University*; Hongxin Hu, *Delaware State University*

**Explicating SDKs: Uncovering Assumptions Underlying Secure Authentication and Authorization** .....399  
Rui Wang, *Microsoft Research Redmond*; Yuchen Zhou, *University of Virginia*; Shuo Chen and Shaz Qadeer, *Microsoft Research Redmond*; David Evans, *University of Virginia*; Yuri Gurevich, *Microsoft Research Redmond*

**Enabling Fine-Grained Permissions for Augmented Reality Applications with Recognizers** .....415  
Suman Jana, *The University of Texas at Austin*; David Molnar and Alexander Moshchuk, *Microsoft Research*; Alan Dunn, *The University of Texas at Austin*; Benjamin Livshits, Helen J. Wang, and Eyal Ofek, *Microsoft Research*

## Hardware and Embedded Security I

**CacheAudit: A Tool for the Static Analysis of Cache Side Channels** .....431  
Goran Doychev, *IMDEA Software Institute*; Dominik Feld, *Saarland University*; Boris Köpf and Laurent Mauborgne, *IMDEA Software Institute*; Jan Reineke, *Saarland University*

**Transparent ROP Exploit Mitigation Using Indirect Branch Tracing** .....447  
Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis, *Columbia University*

**FIE on Firmware: Finding Vulnerabilities in Embedded Systems using Symbolic Execution** .....463  
Drew Davidson, Benjamin Moench, Somesh Jha, and Thomas Ristenpart, *University of Wisconsin—Madison*

## Friday, August 16, 2013

### Hardware and Embedded Security II

**Sancus: Low-cost Trustworthy Extensible Networked Devices with a Zero-software Trusted Computing Base** .....479  
Job Noorman, Pieter Agten, Wilfried Daniels, Raoul Strackx, Anthony Van Herrewewe, Christophe Huygens, Bart Preneel, Ingrid Verbauwhede, and Frank Piessens, *KU Leuven*

**Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation** .....495  
Frank Imeson, Ariq Emtenan, Siddharth Garg, and Mahesh V. Tripunitara, *University of Waterloo*

**KI-Mon: A Hardware-assisted Event-triggered Monitoring Platform for Mutable Kernel Object** .....511  
Hoon Lee, *Korea Advanced Institute of Science and Technology (KAIST)*; HyunGon Moon, *Seoul National University*; DaeHee Jang and Kiwhan Kim, *Korea Advanced Institute of Science and Technology (KAIST)*; Jihoon Lee and Yunheung Paek, *Seoul National University*; Brent ByungHoon Kang, *Korea Advanced Institute of Science and Technology (KAIST)*

(Friday, August 16, continues on p. vi)

## Mobile Security II

**WHYPER: Towards Automating Risk Assessment of Mobile Applications** .....527  
Rahul Pandita, Xusheng Xiao, Wei Yang, William Enck, and Tao Xie, *North Carolina State University*

**Effective Inter-Component Communication Mapping in Android with *Epicc*: An Essential Step Towards Holistic Security Analysis** .....543  
Damien Octeau and Patrick McDaniel, *Pennsylvania State University*; Somesh Jha, *University of Wisconsin*;  
Alexandre Bartel, *University of Luxembourg*; Eric Bodden, *Technische Universität Darmstadt*; Jacques Klein  
and Yves Le Traon, *University of Luxembourg*

**Jekyll on iOS: When Benign Apps Become Evil** .....559  
Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee, *Georgia Institute of Technology*

## Large Scale Systems Security III

**Measuring the Practical Impact of DNSSEC Deployment** .....573  
Wilson Lian, *University of California, San Diego*; Eric Rescorla, *RTFM, Inc.*; Hovav Shacham and Stefan  
Savage, *University of California, San Diego*

**ExecScent: Mining for New C&C Domains in Live Networks with Adaptive Control Protocol Templates** ... 589  
Terry Nelms, *Damballa, Inc. and Georgia Institute of Technology*; Roberto Perdisci, *University of Georgia and  
Georgia Institute of Technology*; Mustaque Ahamad, *Georgia Institute of Technology and New York University  
Abu Dhabi*

**ZMap: Fast Internet-wide Scanning and Its Security Applications** .....605  
Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, *University of Michigan*

## Web Security

**Eradicating DNS Rebinding with the Extended Same-Origin Policy** .....621  
Martin Johns and Sebastian Lekies, *SAP Research*; Ben Stock, *Friedrich-Alexander-Universität  
Erlangen-Nürnberg*

**Revolver: An Automated Approach to the Detection of Evasive Web-based Malware** .....637  
Alexandros Kapravelos and Yan Shoshitaishvili, *University of California, Santa Barbara*; Marco Cova,  
*University of Birmingham*; Christopher Kruegel and Giovanni Vigna, *University of California, Santa Barbara*

**Language-based Defenses against Untrusted Browser Origins** .....653  
Karthikeyan Bhargavan and Antoine Delignat-Lavaud, *INRIA Paris-Rocquencourt*; Sergio Maffei, *Imperial  
College London*

## Attacks

**Take This Personally: Pollution Attacks on Personalized Services** .....671  
Xinyu Xing, Wei Meng, and Dan Doozan, *Georgia Institute of Technology*; Alex C. Snoeren, *University of  
California, San Diego*; Nick Feamster and Wenke Lee, *Georgia Institute of Technology*

**Steal This Movie: Automatically Bypassing DRM Protection in Streaming Media Services** .....687  
Ruoyu Wang, *University of California, Santa Barbara and Tsinghua University*; Yan Shoshitaishvili, Christopher  
Kruegel, and Giovanni Vigna, *University of California, Santa Barbara*