

# 24th USENIX Security Symposium

August 12–14, 2015

Washington, D.C.

Message from the Program Chair . . . . . xi–xii

## Wednesday, August 12

### Measurement: We Didn't Start the Fire

**Post-Mortem of a Zombie: Conficker Cleanup After Six Years.** . . . . . 1  
Hadi Asghari, Michael Ciere, and Michel J.G. van Eeten, *Delft University of Technology*

**Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World.** . . . 17  
Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R.B. Butler, *University of Florida*

**Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.** . . . . . 33  
Kyle Soska and Nicolas Christin, *Carnegie Mellon University*

### Now You're Just Something That I Used to Code

**Under-Constrained Symbolic Execution: Correctness Checking for Real Code** . . . . . 49  
David A. Ramos and Dawson Engler, *Stanford University*

**TaintPipe: Pipelined Symbolic Taint Analysis.** . . . . . 65  
Jiang Ming, Dinghao Wu, Gaoyao Xiao, Jun Wang, and Peng Liu, *The Pennsylvania State University*

**Type Casting Verification: Stopping an Emerging Attack Vector** . . . . . 81  
Byoungyoung Lee, Chengyu Song, Taesoo Kim, and Wenke Lee, *Georgia Institute of Technology*

### Tic-Attack-Toe

**All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS.** . . . . . 97  
Mathy Vanhoef and Frank Piessens, *Katholieke Universiteit Leuven*

**Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS** . . . . . 113  
Christina Garman, *Johns Hopkins University*; Kenneth G. Paterson and Thyla Van der Merwe, *University of London*

**Eclipse Attacks on Bitcoin's Peer-to-Peer Network** . . . . . 129  
Ethan Heilman and Alison Kendler, *Boston University*; Aviv Zohar, *The Hebrew University of Jerusalem and MSR Israel*; Sharon Goldberg, *Boston University*

### Word Crimes

**Compiler-instrumented, Dynamic Secret-Redaction of Legacy Processes for Attacker Deception** . . . . . 145  
Frederico Araujo and Kevin W. Hamlen, *The University of Texas at Dallas*

**Control-Flow Bending: On the Effectiveness of Control-Flow Integrity** . . . . . 161  
Nicolas Carlini, *University of California, Berkeley*; Antonio Barresi, *ETH Zürich*; Mathias Payer, *Purdue University*; David Wagner, *University of California, Berkeley*; Thomas R. Gross, *ETH Zürich*

**Automatic Generation of Data-Oriented Exploits** . . . . . 177  
Hong Hu, Zheng Leong Chua, Sendroiu Adrian, Prateek Saxena, and Zhenkai Liang, *National University of Singapore*

## **Sock It To Me: TLS No Less**

**Protocol State Fuzzing of TLS Implementations** .....193  
Joeri de Ruiter, *University of Birmingham*; Erik Poll, *Radboud University Nijmegen*

**Verified Correctness and Security of OpenSSL HMAC** .....207  
Lennart Beringer, *Princeton University*; Adam Petcher, *Harvard University and MIT Lincoln Laboratory*;  
Katherine Q. Ye and Andrew W. Appel, *Princeton University*

**Not-Quite-So-Broken TLS: Lessons in Re-Engineering a Security Protocol Specification  
and Implementation** ..... 223  
David Kaloper-Meršinjak, Hannes Mehnert, Anil Madhavapeddy, and Peter Sewell, *University of Cambridge*

**To Pin or Not to Pin—Helping App Developers Bullet Proof Their TLS Connections** .....239  
Marten Oltrogge and Yasemin Acar, *Leibniz Universität Hannover*; Sergej Dechand and Matthew Smith,  
*Universität Bonn*; Sascha Fahl, *Fraunhofer FKIE*

## **Forget Me Not**

**De-anonymizing Programmers via Code Stylometry** .....255  
Aylin Caliskan-Islam, *Drexel University*; Richard Harang, *U.S. Army Research Laboratory*; Andrew Liu,  
*University of Maryland*; Arvind Narayanan, *Princeton University*; Clare Voss, *U.S. Army Research Laboratory*;  
Fabian Yamaguchi, *University of Goettingen*; Rachel Greenstadt, *Drexel University*

**RAPTOR: Routing Attacks on Privacy in Tor** .....271  
Yixin Sun and Anne Edmundson, *Princeton University*; Laurent Vanbever, *ETH Zürich*; Oscar Li, Jennifer  
Rexford, Mung Chiang, and Prateek Mittal, *Princeton University*

**Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services** .....287  
Albert Kwon, *Massachusetts Institute of Technology*; Mashael AlSabah, *Qatar Computing Research Institute,  
Qatar University, and Massachusetts Institute of Technology*; David Lazar, *Massachusetts Institute of  
Technology*; Marc Dacier, *Qatar Computing Research Institute*; Srinivas Devadas, *Massachusetts Institute  
of Technology*

**SecGraph: A Uniform and Open-source Evaluation System for Graph Data Anonymization  
and De-anonymization** .....303  
Shouling Ji and Weiqing Li, *Georgia Institute of Technology*; Prateek Mittal, *Princeton University*;  
Xin Hu, *IBM T. J. Watson Research Center*; Raheem Beyah, *Georgia Institute of Technology*

## **Thursday, August 13**

### **Operating System Security: It's All About the Base**

**Trustworthy Whole-System Provenance for the Linux Kernel** .....319  
Adam Bates, Dave (Jing) Tian, and Kevin R.B. Butler, *University of Florida*; Thomas Moyer,  
*MIT Lincoln Laboratory*

**Securing Self-Virtualizing Ethernet Devices** .....335  
Igor Smolyar, Muli Ben-Yehuda, and Dan Tsafir, *Technion—Israel Institute of Technology*

**EASEAndroid: Automatic Policy Analysis and Refinement for Security Enhanced Android via  
Large-Scale Semi-Supervised Learning** .....351  
Ruowen Wang, *Samsung Research America and North Carolina State University*; William Enck and Douglas  
Reeves, *North Carolina State University*; Xinwen Zhang, *Samsung Research America*; Peng Ning, *Samsung  
Research America and North Carolina State University*; Dingbang Xu, Wu Zhou, and Ahmed M. Azab,  
*Samsung Research America*

(Thursday, August 13, continues on next page)

## **Ace Ventura: PETS Detective**

**Marionette: A Programmable Network Traffic Obfuscation System** .....367  
Kevin P. Dyer, *Portland State University*; Scott E. Coull, *RedJack LLC.*; Thomas Shrimpton, *Portland State University*

**CONIKS: Bringing Key Transparency to End Users** .....383  
Marcela S. Melara and Aaron Blankstein, *Princeton University*; Joseph Bonneau, *Stanford University and The Electronic Frontier Foundation*; Edward W. Felten and Michael J. Freedman, *Princeton University*

**Investigating the Computer Security Practices and Needs of Journalists** .....399  
Susan E. McGregor, *Columbia Journalism School*; Polina Charters, Tobin Holliday, and Franziska Roesner, *University of Washington*

## **ORAMorama!**

**Constants Count: Practical Improvements to Oblivious RAM** .....415  
Ling Ren, Christopher Fletcher, and Albert Kwon, *Massachusetts Institute of Technology*; Emil Stefanov, *University of California, Berkeley*; Elaine Shi, *Cornell University*; Marten van Dijk, *University of Connecticut*; Srinivas Devadas, *Massachusetts Institute of Technology*

**Raccoon: Closing Digital Side-Channels through Obfuscated Execution** .....431  
Ashay Rane, Calvin Lin, and Mohit Tiwari, *The University of Texas at Austin*

**M2R: Enabling Stronger Privacy in MapReduce Computation** .....447  
Tien Tuan Anh Dinh, Prateek Saxena, Ee-Chien Chang, Beng Chin Ooi, and Chunwang Zhang, *National University of Singapore*

## **But Maybe All You Need Is Something to Trust**

**Measuring Real-World Accuracies and Biases in Modeling Password Guessability** .....463  
Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, and Darya Kurilova, *Carnegie Mellon University*; Michelle L. Mazurek, *University of Maryland*; William Melicher and Richard Shay, *Carnegie Mellon University*

**Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound** .....483  
Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Čapkun, *ETH Zürich*

**Android Permissions Remystified: A Field Study on Contextual Integrity** .....499  
Primal Wijesekera, *University of British Columbia*; Arjun Baokar, Ashkan Hosseini, Serge Egelman, and David Wagner, *University of California, Berkeley*; Konstantin Beznosov, *University of British Columbia*

## **PELCGB**

**Phasing: Private Set Intersection using Permutation-based Hashing** .....515  
Benny Pinkas, *Bar-Ilan University*; Thomas Schneider, *Technische Universität Darmstadt*; Gil Segev, *The Hebrew University of Jerusalem*; Michael Zohner, *Technische Universität Darmstadt*

**Faster Secure Computation through Automatic Parallelization** .....531  
Niklas Buescher and Stefan Katzenbeisser, *Technische Universität Darmstadt*

**The Pythia PRF Service** .....547  
Adam Everspaugh and Rahul Chaterjee, *University of Wisconsin—Madison*; Samuel Scott, *University of London*; Ari Juels and Thomas Ristenpart, *Cornell Tech*

## **And the Hackers Gonna Hack, Hack, Hack, Hack, Hack**

**EVILCOHORT: Detecting Communities of Malicious Accounts on Online Services . . . . .563**  
Gianluca Stringhini, *University College London*; Pierre Moulranne, *University of California, Santa Barbara*;  
Gregoire Jacob, *Lastline Inc.*; Manuel Egele, *Boston University*; Christopher Kruegel and Giovanni Vigna,  
*University of California, Santa Barbara*

**Trends and Lessons from Three Years Fighting Malicious Extensions. . . . .579**  
Nav Jagpal, Eric Dingle, Jean-Philippe Gravel, Panayiotis Mavrommatis, Niels Provos, Moheeb Abu Rajab,  
and Kurt Thomas, *Google*

**Meerkat: Detecting Website Defacements through Image-based Object Recognition. . . . .595**  
Kevin Borgolte, Christopher Kruegel, and Giovanni Vigna, *University of California, Santa Barbara*

## **It's a Binary Joke: Either You Get It, or You Don't**

**Recognizing Functions in Binaries with Neural Networks . . . . .611**  
Eui Chul Richard Shin, Dawn Song, and Reza Moazzezi, *University of California, Berkeley*

**Reassembleable Disassembling . . . . .627**  
Shuai Wang, Pei Wang, and Dinghao Wu, *The Pennsylvania State University*

**How the ELF Ruined Christmas . . . . .643**  
Alessandro Di Federico, *University of California, Santa Barbara and Politecnico di Milano*; Amat Cama,  
Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna, *University of California, Santa Barbara*

## **Friday, August 14**

### **Pain in the App**

**Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale. . . . .659**  
Kai Chen, *Chinese Academy of Sciences and Indiana University*; Peng Wang, Yeonjoon Lee, Xiaofeng Wang,  
and Nan Zhang, *Indiana University*; Heqing Huang, *The Pennsylvania State University*; Wei Zou, *Chinese*  
*Academy of Sciences*; Peng Liu, *The Pennsylvania State University*

**You Shouldn't Collect My Secrets: Thwarting Sensitive Keystroke Leakage in Mobile IME Apps. . . . .675**  
Jin Chen and Haibo Chen, *Shanghai Jiao Tong University*; Erick Bauman and Zhiqiang Lin, *The University*  
*of Texas at Dallas*; Binyu Zang and Haibing Guan, *Shanghai Jiao Tong University*

**Boxify: Full-fledged App Sandboxing for Stock Android. . . . .691**  
Michael Backes, *Saarland University and Max Planck Institute for Software Systems (MPI-SWS)*; Sven Bugiel,  
Christian Hammer, Oliver Schranz, and Philipp von Styp-Rekowsky, *Saarland University*

### **Oh, What a Tangled Web We Weave**

**Cookies Lack Integrity: Real-World Implications. . . . .707**  
Xiaofeng Zheng, *Tsinghua University and Tsinghua National Laboratory for Information Science and*  
*Technology*; Jian Jiang, *University of California, Berkeley*; Jinjin Liang, *Tsinghua University and Tsinghua*  
*National Laboratory for Information Science and Technology*; Haixin Duan, *Tsinghua University, Tsinghua*  
*National Laboratory for Information Science and Technology, and International Computer Science Institute*;  
Shuo Chen, *Microsoft Research Redmond*; Tao Wan, *Huawei Canada*; Nicholas Weaver, *International Computer*  
*Science Institute and University of California, Berkeley*

**The Unexpected Dangers of Dynamic JavaScript . . . . .723**  
Sebastian Lekies, *Ruhr-University Bochum*; Ben Stock, *Friedrich-Alexander-Universität Erlangen-Nürnberg*;  
Martin Wentzel and Martin Johns, *SAP SE*

**ZigZag: Automatically Hardening Web Applications Against Client-side Validation Vulnerabilities. . . . .737**  
Michael Weissbacher, William Robertson, and Engin Kirda, *Northeastern University*; Christopher Kruegel and  
Giovanni Vigna, *University of California, Santa Barbara*

(Friday, August 14, continues on next page)

## **The World's Address: An App That's Worn**

**Anatomization and Protection of Mobile Apps' Location Privacy Threats** .....753  
Kassem Fawaz, Huan Feng, and Kang G. Shin, *University of Michigan*

**LinkDroid: Reducing Unregulated Aggregation of App Usage Behaviors** .....769  
Huan Feng, Kassem Fawaz, and Kang G. Shin, *University of Michigan*

**PowerSpy: Location Tracking using Mobile Device Power Analysis** .....785  
Yan Michalevsky, Aaron Schulman, Gunaa Arumugam Veerapandian, and Dan Boneh, *Stanford University*;  
Gabi Nakibly, *National Research and Simulation Center/Rafael Ltd.*

## **ADDioS!**

**In the Compression Hornet's Nest: A Security Study of Data Compression in Network Services** .....801  
Giancarlo Pellegrino, *Saarland University*; Davide Balzarotti, *Eurecom*; Stefan Winter and Neeraj Suri,  
*Technische Universität Darmstadt*

**Bohatei: Flexible and Elastic DDoS Defense** .....817  
Seyed K. Fayaz, Yoshiaki Tobioka, and Vyas Sekar, *Carnegie Mellon University*; Michael Bailey, *University of Illinois at Urbana-Champaign*

**Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge** .....833  
Bradley Reaves, *University of Florida*; Ethan Shernan, *Georgia Institute of Technology*; Adam Bates,  
*University of Florida*; Henry Carter, *Georgia Institute of Technology*; Patrick Traynor, *University of Florida*

## **Attacks: I Won't Let You Down**

**GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies** .....849  
Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici, *Ben-Gurion University of the Negev*

**Thermal Covert Channels on Multi-core Platforms** .....865  
Ramya Jayaram Masti, Devendra Rai, Aanjan Ranganathan, Christian Müller, Lothar Thiele, and  
Srdjan Čapkun, *ETH Zürich*

**Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors** .....881  
Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi,  
and Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*

## **How Do You Secure a Cloud and Pin it Down?**

**Cache Template Attacks: Automating Attacks on Inclusive Last-Level Caches** .....897  
Daniel Gruss, Raphael Spreitzer, and Stefan Mangard, *Graz University of Technology*

**A Placement Vulnerability Study in Multi-Tenant Public Clouds** .....913  
Venkatanathan Varadarajan, *University of Wisconsin—Madison*; Yinqian Zhang, *The Ohio State University*;  
Thomas Ristenpart, *Cornell Tech*; Michael Swift, *University of Wisconsin—Madison*

**A Measurement Study on Co-residence Threat inside the Cloud** .....929  
Zhang Xu, *College of William and Mary*; Haining Wang, *University of Delaware*; Zhenyu Wu,  
*NEC Laboratories America*

## **Knock Knock. Who's There? Icy. Icy who? I See You Too**

**Towards Discovering and Understanding Task Hijacking in Android** .....945

Chuangang Ren, *The Pennsylvania State University*; Yulong Zhang, Hui Xue, and Tao Wei, *Fireeye, Inc.*;  
Peng Liu, *The Pennsylvania State University*

**Cashtags: Protecting the Input and Display of Sensitive Data** .....961

Michael Mitchell and An-I Andy Wang, *Florida State University*; Peter Reiher, *University of California, Los Angeles*

**SUPOR: Precise and Scalable Sensitive User Input Detection for Android Apps** .....977

Jianjun Huang, *Purdue University*; Zhichun Li, Xusheng Xiao, and Zhenyu Wu, *NEC Labs America*; Kangjie Lu, *Georgia Institute of Technology*; Xiangyu Zhang, *Purdue University*; Guofei Jiang, *NEC Labs America*

**UIPicker: User-Input Privacy Identification in Mobile Applications** .....993

Yuhong Nan, Min Yang, Zhemin Yang, and Shunfan Zhou, *Fudan University*; Guofei Gu, *Texas A&M University*; Xiaofeng Wang, *Indiana University Bloomington*

## **How Do You Solve a Problem Like M-al-ware?**

**Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents** .....1009

Yang Liu, Armin Sarabi, Jing Zhang, and Parinaz Naghizadeh, *University of Michigan*; Manish Karir, *QuadMetrics, Inc.*; Michael Bailey, *University of Illinois at Urbana-Champaign*; Mingyan Liu, *University of Michigan and QuadMetrics, Inc.*

**WebWitness: Investigating, Categorizing, and Mitigating Malware Download Paths** .....1025

Terry Nelms, *Damballa, Inc. and Georgia Institute of Technology*; Roberto Perdisci, *University of Georgia and Georgia Institute of Technology*; Manos Antonakakis, *Georgia Institute of Technology*; Mustaque Ahamad, *Georgia Institute of Technology and New York University Abu Dhabi*

**Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting**

**Real-World Exploits** .....1041

Carl Sabottke, Octavian Suciu, and Tudor Dumitras, *University of Maryland*

**Needles in a Haystack: Mining Information from Public Dynamic Analysis Sandboxes for**

**Malware Intelligence** .....1057

Mariano Graziano and Davide Canali, *Eurecom*; Leyla Bilge, *Symantec Research Labs*; Andrea Lanzi, *Università degli Studi di Milano*; Davide Balzarotti, *Eurecom*

The Supplement to the Proceedings of the 22nd USENIX Security Symposium follows.