

18th USENIX Security Symposium
August 10–14, 2009
San Jose, CA, USA

Index of Authors vi
Message from the Program Chair vii

Wednesday, August 12

Attacks on Privacy

Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. 1
Martin Vuagnoux and Sylvain Pasini, LASEC/EPFL

Peeping Tom in the Neighborhood: Keystroke Eavesdropping on Multi-User Systems. 17
Kehuan Zhang and XiaoFeng Wang, Indiana University, Bloomington

A Practical Congestion Attack on Tor Using Long Paths 33
Nathan S. Evans, University of Denver; Roger Dingledine, The Tor Project; Christian Grothoff, University of Denver

Memory Safety

Baggy Bounds Checking: An Efficient and Backwards-Compatible Defense against Out-of-Bounds Errors 51
Periklis Akrkitidis, Computer Laboratory, University of Cambridge; Manuel Costa and Miguel Castro, Microsoft Research, Cambridge; Steven Hand, Computer Laboratory, University of Cambridge

Dynamic Test Generation to Find Integer Bugs in x86 Binary Linux Programs 67
David Molnar, Xue Cong Li, and David A. Wagner, University of California, Berkeley

Memory Safety for Low-Level Software/Hardware Interactions 83
John Criswell, University of Illinois; Nicolas Geoffray, Université Pierre et Marie Curie, INRIA/Regal; Vikram Adve, University of Illinois

Network Security

Detecting Spammers with SNARE: Spatio-temporal Network-level Automatic Reputation Engine. 101
Shuang Hao, Nadeem Ahmed Syed, Nick Feamster, and Alexander G. Gray, Georgia Tech; Sven Krasser, McAfee, Inc.

Improving Tor using a TCP-over-DTLS Tunnel 119
Joel Reardon, Google Switzerland GmbH; Ian Goldberg, University of Waterloo

Locating Prefix Hijackers using LOCK. 135
Tongqing Qiu, Georgia Tech; Lusheng Ji, Dan Pei, and Jia Wang, AT&T Labs—Research; Jun (Jim) Xu, Georgia Tech; Hitesh Ballani, Cornell University

Thursday, August 13

JavaScript Security

- GATEKEEPER: Mostly Static Enforcement of Security and Reliability Policies for JavaScript Code 151
Salvatore Guarnieri, University of Washington; Benjamin Livshits, Microsoft Research
- NOZZLE: A Defense Against Heap-spraying Code Injection Attacks 169
Paruj Ratanaworabhan, Cornell University; Benjamin Livshits and Benjamin Zorn, Microsoft Research
- Cross-Origin JavaScript Capability Leaks: Detection, Exploitation, and Defense 187
Adam Barth, Joel Weinberger, and Dawn Song, University of California, Berkeley

Radio

- Physical-layer Identification of RFID Devices 199
Boris Danev, ETH Zürich, Switzerland; Thomas S. Heydt-Benjamin, IBM Zürich Research Laboratory, Switzerland; Srdjan Capkun, ETH Zürich, Switzerland
- CCCP: Secure Remote Storage for Computational RFIDs 215
Mastoreh Salajegheh, Shane Clark, Benjamin Ransford, and Kevin Fu, University of Massachusetts Amherst; Ari Juels, RSA Laboratories, The Security Division of EMC
- Jamming-resistant Broadcast Communication without Shared Keys 231
Christina Pöpper, Mario Strasser, and Srdjan Capkun, ETH Zürich, Switzerland

Securing Web Apps

- xBook: Redesigning Privacy Control in Social Networking Platforms 249
Kapil Singh, Georgia Institute of Technology; Sumeer Bhola, Google; Wenke Lee, Georgia Institute of Technology
- Nemesis: Preventing Authentication & Access Control Vulnerabilities in Web Applications 267
Michael Dalton and Christos Kozyrakis, Stanford University; Nikolai Zeldovich, CSAIL, MIT
- Static Enforcement of Web Application Integrity Through Strong Typing 283
William Robertson and Giovanni Vigna, University of California, Santa Barbara

Applied Crypto

- Vanish: Increasing Data Privacy with Self-Destructing Data 299
Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy, and Henry M. Levy, University of Washington
- Efficient Data Structures For Tamper-Evident Logging 317
Scott A. Crosby and Dan S. Wallach, Rice University
- VPriv: Protecting Privacy in Location-Based Vehicular Services 335
Raluca Ada Popa and Hari Balakrishnan, Massachusetts Institute of Technology; Andrew J. Blumberg, Stanford University

Friday, August 14

Malware Detection and Protection

- Effective and Efficient Malware Detection at the End Host 351
Clemens Kolbitsch and Paolo Milani Comparetti, Secure Systems Lab, TU Vienna; Christopher Kruegel, University of California, Santa Barbara; Engin Kirda, Institute Eurecom, Sophia Antipolis; Xiaoyong Zhou and XiaoFeng Wang, Indiana University at Bloomington
- Protecting Confidential Data on Personal Computers with Storage Capsules 367
Kevin Borders, Eric Vander Weele, Billy Lau, and Atul Prakash, University of Michigan
- Return-Oriented Rootkits: Bypassing Kernel Code Integrity Protection Mechanisms 383
Ralf Hund, Thorsten Holz, and Felix C. Freiling, Laboratory for Dependable Distributed Systems, University of Mannheim, Germany

Browser Security

- Crying Wolf: An Empirical Study of SSL Warning Effectiveness 399
Joshua Sunshine, Serge Egelman, Hazim Almuhtedi, Neha Atri, and Lorrie Faith Cranor, Carnegie Mellon University
- The Multi-Principal OS Construction of the Gazelle Web Browser 417
Helen J. Wang, Microsoft Research; Chris Grier, University of Illinois at Urbana-Champaign; Alex Moshchuk, University of Washington; Samuel T. King, University of Illinois at Urbana-Champaign; Piali Choudhury and Herman Venter, Microsoft Research

Index of Authors

- Adve, Vikram, 83
Ahmed Syed, Nadeem, 101
Akritidis, Periklis, 51
Almuhimedi, Hazim, 399
Atri, Neha, 399
Balakrishnan, Hari, 335
Ballani, Hitesh, 135
Barth, Adam, 187
Bhola, Sumeer, 249
Blumberg, Andrew J., 335
Borders, Kevin, 367
Capkun, Srdjan, 199, 231
Castro, Miguel, 51
Choudhury, Piali, 417
Clark, Shane, 215
Costa, Manuel, 51
Cranor, Lorrie Faith, 399
Criswell, John, 83
Crosby, Scott A., 317
Dalton, Michael, 267
Danev, Boris, 199
Dingledine, Roger, 33
Egelman, Serge, 399
Evans, Nathan S., 33
Feamster, Nick, 101
Freiling, Felix C., 383
Fu, Kevin, 215
Geambasu, Roxana, 299
Geoffray, Nicolas, 83
Goldberg, Ian, 119
Gray, Alexander G., 101
Grier, Chris, 417
Grothoff, Christian, 33
Guarnieri, Salvatore, 151
Hand, Steven, 51
Hao, Shuang, 101
Heydt-Benjamin, Thomas S., 199
Holz, Thorsten, 383
Hund, Ralf, 383
Ji, Lusheng, 135
Juels, Ari, 215
King, Samuel T., 417
Kirda, Engin, 351
Kohno, Tadayoshi, 299
Kolbitsch, Clemens, 351
Kozyrakakis, Christos, 267
Krasser, Sven, 101
Kruegel, Christopher, 351
Lau, Billy, 367
Lee, Wenke, 249
Levy, Amit A., 299
Levy, Henry M., 299
Li, Xue Cong, 67
Livshits, Benjamin, 151, 169
Milani Comparetti, Paolo, 351
Molnar, David, 67
Moshchuk, Alex, 417
Pasini, Sylvain, 1
Pei, Dan, 135
Popa, Raluca Ada, 335
Pöpper, Christina, 231
Prakash, Atul, 367
Qiu, Tongqing, 135
Ransford, Benjamin, 215
Ratanaworabhan, Paruj, 169
Reardon, Joel, 119
Robertson, William, 283
Salajegheh, Mastrooreh, 215
Singh, Kapil, 249
Song, Dawn, 187
Strasser, Mario, 231
Sunshine, Joshua, 399
Vander Weele, Eric, 367
Venter, Herman, 417
Vigna, Giovanni, 283
Vuagnoux, Martin, 1
Wagner, David A., 67
Wallach, Dan S., 317
Wang, Helen J., 417
Wang, Jia, 135
Wang, XiaoFeng, 17, 351
Weinberger, Joel, 187
Xu, Jun (Jim), 135
Zeldovich, Nickolai, 267
Zhang, Kehuan, 17
Zhou, Xiaoyong, 351
Zorn, Benjamin, 169