20th USENIX Security Symposium
August 8–12, 2011
San Francisco, CA, USA

Message from the USENIX Security ’11 Program Chair vii

Wednesday, August 10

Web Security

Fast and Precise Sanitizer Analysis with BEK 1
Pieter Hooimeijer, University of Virginia; Benjamin Livshits and David Molnar, Microsoft Research; Prateek Saxena, University of California, Berkeley; Margus Veanes, Microsoft Research

Toward Secure Embedded Web Interfaces. 17
Baptiste Gourdin, LSV ENS-Cachan; Chinmay Soman, Hristo Bojinov, and Elie Bursztein, Stanford University

ZOZZLE: Fast and Precise In-Browser JavaScript Malware Detection 33
Charlie Curtsinger, University of Massachusetts Amherst; Benjamin Livshits and Benjamin Zorn, Microsoft Research; Christian Seifert, Microsoft

Analysis of Deployed Systems

Why (Special Agent) Johnny (Still) Can’t Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System 49
Sandy Clark, Travis Goodspeed, Perry Metzger, Zachary Wasserman, Kevin Xu, and Matt Blaze, University of Pennsylvania

Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space 65
Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar Weippl, SBA Research

Comprehensive Experimental Analyses of Automotive Attack Surfaces 77
Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, University of California, San Diego; Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, University of Washington

Forensic Analysis

Forensic Triage for Mobile Phones with DEC0DE 93
Robert J. Walls, Erik Learned-Miller, and Brian Neil Levine, University of Massachusetts Amherst

mCarve: Carving Attributed Dump Sets 107
Ton van Deursen, Sjouke Mauw, and Saša Radomirović, University of Luxembourg

SHELLOS: Enabling Fast Detection and Forensic Analysis of Code Injection Attacks 123
Kevin Z. Snow, Srinivas Krishnan, and Fabian Monrose, University of North Carolina at Chapel Hill; Niels Provos, Google

Thursday, August 11

Static and Dynamic Analysis

MACE: Model-inference-Assisted Concolic Exploration for Protocol and Vulnerability Discovery . . . 139
Chia Yuan Cho, University of California, Berkeley, and DSO National Labs; Domagoj Babić, University of California, Berkeley; Pongsin Poosankam, University of California, Berkeley, and Carnegie Mellon University; Kevin Zhijie Chen, Edward XueJun Wu, and Dawn Song, University of California, Berkeley

Static Detection of Access Control Vulnerabilities in Web Applications . . . 155
Fangqi Sun, Liang Xu, and Zhendong Su, University of California, Davis

ADsafety: Type-Based Verification of JavaScript Sandboxing . . . 171
Joe Gibbs Politz, Spiridon Aristides Eliopoulos, Arjun Guha, and Shriram Krishnamurthi, Brown University

Understanding the Underground Economy

Measuring *Pay-per-Install*: The Commoditization of Malware Distribution . . . 187
Juan Caballero, IMDEA Software Institute; Chris Grier, Christian Kreibich, and Vern Paxson, University of California, Berkeley, and ICSI

Dirty Jobs: The Role of Freelance Labor in Web Service Abuse . . . 203
Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker, University of California, San Diego

Show Me the Money: Characterizing Spam-advertised Revenue . . . 219
Chris Kanich, University of California, San Diego; Nicholas Weaver, International Computer Science Institute; Damon McCoy and Tristan Halvorson, University of California, San Diego; Christian Kreibich, International Computer Science Institute; Kirill Levchenko, University of California, San Diego; Vern Paxson, International Computer Science Institute and University of California, Berkeley; Geoffrey M. Voelker and Stefan Savage, University of California, San Diego

Defenses and New Directions

Secure In-Band Wireless Pairing . . . 235
Shyamnath Gollakota, Nabeel Ahmed, Nickolai Zeldovich, and Dina Katabi, Massachusetts Institute of Technology

TRESOR Runs Encryption Securely Outside RAM . . . 251
Tilo Müller and Felix C. Freiling, University of Erlangen; Andreas Dewald, University of Mannheim

Bubble Trouble: Off-Line De-Anonymization of Bubble Forms . . . 267
Joseph A. Calandrino, William Clarkson, and Edward W. Felten, Princeton University

Securing Search

Measuring and Analyzing Search-Redirection Attacks in the Illicit Online Prescription Drug Trade . . . 281
Nektarios Leontiadis, Carnegie Mellon University; Tyler Moore, Harvard University; Nicolas Christin, Carnegie Mellon University

deSEO: Combating Search-Result Poisoning . . . 299
John P. John, University of Washington; Fang Yu and Yinglian Xie, MSR Silicon Valley; Arvind Krishnamurthy, University of Washington; Martín Abadi, MSR Silicon Valley

Thursday, August 11 (continued)

Securing Smart Phones

A Study of Android Application Security . . . 315
William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri, The Pennsylvania State University

Permission Re-Delegation: Attacks and Defenses . . . 331
Adrienne Porter Felt, University of California, Berkeley; Helen J. Wang and Alexander Moshchuk, Microsoft Research; Steve Hanna and Erika Chin, University of California, Berkeley

QUIRE: Lightweight Provenance for Smart Phone Operating Systems . . . 347
Michael Dietz, Shashi Shekhar, Yuliy Pisetsky, Anhei Shu, and Dan S. Wallach, Rice University

Friday, August 12

Understanding Attacks

SMS of Death: From Analyzing to Attacking Mobile Phones on a Large Scale . . . 363
Collin Mulliner, Nico Golde, and Jean-Pierre Seifert, Technische Universität Berlin and Deutsche Telekom Laboratories

Q: Exploit Hardening Made Easy . . . 379
Edward J. Schwartz, Thanassis Avgerinos, and David Brumley, Carnegie Mellon University

Cloaking Malware with the Trusted Platform Module . . . 395
Alan M. Dunn, Owen S. Hofmann, Brent Waters, and Emmett Witchel, The University of Texas at Austin

Dealing with Malware and Bots

Detecting Malware Domains at the Upper DNS Hierarchy . . . 411
Manos Antonakakis, Damballa Inc. and Georgia Institute of Technology; Roberto Perdisci, University of Georgia; Wenke Lee, Georgia Institute of Technology; Nikolaos Vasiloglou II, Damballa Inc.; David Dagon, Georgia Institute of Technology

BOTMAGNIFIER: Locating Spambots on the Internet . . . 427
Gianluca Stringhini, University of California, Santa Barbara; Thorsten Holz, Ruhr-University Bochum; Brett Stone-Gross, Christopher Kruegel, and Giovanni Vigna, University of California, Santa Barbara

JACKSTRAWS: Picking Command and Control Connections from Bot Traffic . . . 443
Gregoire Jacob, University of California, Santa Barbara; Ralf Hund, Ruhr-University Bochum; Christopher Kruegel, University of California, Santa Barbara; Thorsten Holz, Ruhr-University Bochum

(Friday, August 12, continues on p. vi)

Friday, August 12 (continued)

Privacy- and Freedom-Enhancing Technologies

Telex: Anticensorship in the Network Infrastructure 459
Eric Wustrow and Scott Wolchok, The University of Michigan; Ian Goldberg, University of Waterloo; J. Alex Halderman, The University of Michigan

PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval 475
Prateek Mittal, University of Illinois at Urbana-Champaign; Femi Olumofin, University of Waterloo; Carmela Troncoso, K.U.Leuven/IBBT; Nikita Borisov, University of Illinois at Urbana-Champaign; Ian Goldberg, University of Waterloo

The Phantom Tollbooth: Privacy-Preserving Electronic Toll Collection in the Presence of Driver Collusion 491
Sarah Meiklejohn, Keaton Mowery, Stephen Checkoway, and Hovav Shacham, University of California, San Diego

Applied Cryptography

Differential Privacy Under Fire 507
Andreas Haeberlen, Benjamin C. Pierce, and Arjun Narayan, University of Pennsylvania

Outsourcing the Decryption of ABE Ciphertexts 523
Matthew Green and Susan Hohenberger, Johns Hopkins University; Brent Waters, University of Texas at Austin

Faster Secure Two-Party Computation Using Garbled Circuits 539
Yan Huang and David Evans, University of Virginia; Jonathan Katz, University of Maryland; Lior Malka, Intel