

23rd USENIX Security Symposium
August 20–22, 2014
San Diego, CA

Message from the Program Chair ix

Wednesday, August 20, 2014

Privacy

Privee: An Architecture for Automatically Analyzing Web Privacy Policies.....1
Sebastian Zimmeck and Steven M. Bellovin, *Columbia University*

Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing.....17
Matthew Fredrikson, Eric Lantz, and Somesh Jha, *University of Wisconsin—Madison*; Simon Lin, *Marshfield Clinic Research Foundation*; David Page and Thomas Ristenpart, *University of Wisconsin—Madison*

Mimesis Aegis: A Mimicry Privacy Shield—A System’s Approach to Data Privacy on Public Cloud33
Billy Lau, Simon Chung, Chengyu Song, Yeongjin Jang, Wenke Lee, and Alexandra Boldyreva, *Georgia Institute of Technology*

XRy: Enhancing the Web’s Transparency with Differential Correlation.....49
Mathias Lécuyer, Guillaume Ducoffe, Francis Lan, Andrei Papancea, Theofilos Petsios, Riley Spahn, Augustin Chaintreau, and Roxana Geambasu, *Columbia University*

Mass Pwnage

An Internet-Wide View of Internet-Wide Scanning65
Zakir Durumeric, Michael Bailey, and J. Alex Halderman, *University of Michigan*

On the Feasibility of Large-Scale Infections of iOS Devices79
Tielei Wang, Yeongjin Jang, Yizheng Chen, Simon Chung, Billy Lau, and Wenke Lee, *Georgia Institute of Technology*

A Large-Scale Analysis of the Security of Embedded Firmwares.....95
Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti, *Eurecom*

Exit from Hell? Reducing the Impact of Amplification DDoS Attacks.....111
Marc Kühner, Thomas Hupperich, Christian Rossow, and Thorsten Holz, *Ruhr-University Bochum*

Privacy Enhancing Technology

Never Been KIST: Tor’s Congestion Management Blossoms with Kernel-Informed Socket Transport.....127
Rob Jansen, *U.S. Naval Research Laboratory*; John Geddes, *University of Minnesota*; Chris Wacek and Micah Sherr, *Georgetown University*; Paul Syverson, *U.S. Naval Research Laboratory*

Effective Attacks and Provable Defenses for Website Fingerprinting.....143
Tao Wang, *University of Waterloo*; Xiang Cai, Rishab Nithyanand, and Rob Johnson, *Stony Brook University*; Ian Goldberg, *University of Waterloo*

TapDance: End-to-Middle Anticensorship without Flow Blocking.....159
Eric Wustrow, Colleen M. Swanson, and J. Alex Halderman, *University of Michigan*

A Bayesian Approach to Privacy Enforcement in Smartphones175
Omer Tripp, *IBM Research, USA*; Julia Rubin, *IBM Research, Israel*

Crime and Pun.../Measure-ment

The Long “Taile” of Typosquatting Domain Names	191
Janos Szurdi, <i>Carnegie Mellon University</i> ; Balazs Kocso and Gabor Cseh, <i>Budapest University of Technology and Economics</i> ; Jonathan Spring, <i>Carnegie Mellon University</i> ; Mark Felegyhazi, <i>Budapest University of Technology and Economics</i> ; Chris Kanich, <i>University of Illinois at Chicago</i>	
Understanding the Dark Side of Domain Parking	207
Sumayah Alrwais, <i>Indiana University Bloomington and King Saud University</i> ; Kan Yuan, <i>Indiana University Bloomington</i> ; Eihal Alowaisheq, <i>Indiana University Bloomington and King Saud University</i> ; Zhou Li, <i>Indiana University Bloomington and RSA Laboratories</i> ; XiaoFeng Wang, <i>Indiana University Bloomington</i>	
Towards Detecting Anomalous User Behavior in Online Social Networks	223
Bimal Viswanath and M. Ahmad Bashir, <i>Max Planck Institute for Software Systems (MPI-SWS)</i> ; Mark Crovella, <i>Boston University</i> ; Saikat Guha, <i>Microsoft Research</i> ; Krishna P. Gummadi, <i>Max Planck Institute for Software Systems (MPI-SWS)</i> ; Balachander Krishnamurthy, <i>AT&T Labs–Research</i> ; Alan Mislove, <i>Northeastern University</i>	
Man vs. Machine: Practical Adversarial Detection of Malicious Crowdsourcing Workers	239
Gang Wang, <i>University of California, Santa Barbara</i> ; Tianyi Wang, <i>University of California, Santa Barbara and Tsinghua University</i> ; Haitao Zheng and Ben Y. Zhao, <i>University of California, Santa Barbara</i>	

Thursday, August 21, 2014

Forensics

DSCRETE: Automatic Rendering of Forensic Information from Memory Images via Application Logic Reuse	255
Brendan Saltaformaggio, Zhongshu Gu, Xiangyu Zhang, and Dongyan Xu, <i>Purdue University</i>	
Cardinal Pill Testing of System Virtual Machines	271
Hao Shi, Abdulla Alwabel, and Jelena Mirkovic, <i>USC Information Sciences Institute (ISI)</i>	
BareCloud: Bare-metal Analysis-based Evasive Malware Detection	287
Dhilung Kirat, Giovanni Vigna, and Christopher Kruegel, <i>University of California, Santa Barbara</i>	
Blanket Execution: Dynamic Similarity Testing for Program Binaries and Components	303
Manuel Egele, Maverick Woo, Peter Chapman, and David Brumley, <i>Carnegie Mellon University</i>	

Attacks and Transparency

On the Practical Exploitability of Dual EC in TLS Implementations	319
Stephen Checkoway, <i>Johns Hopkins University</i> ; Matthew Fredrikson, <i>University of Wisconsin–Madison</i> ; Ruben Niederhagen, <i>Technische Universiteit Eindhoven</i> ; Adam Everspaugh, <i>University of Wisconsin–Madison</i> ; Matthew Green, <i>Johns Hopkins University</i> ; Tanja Lange, <i>Technische Universiteit Eindhoven</i> ; Thomas Ristenpart, <i>University of Wisconsin–Madison</i> ; Daniel J. Bernstein, <i>Technische Universiteit Eindhoven and University of Illinois at Chicago</i> ; Jake Maskiewicz and Hovav Shacham, <i>University of California, San Diego</i>	
iSeeYou: Disabling the MacBook Webcam Indicator LED	337
Matthew Brouck and Stephen Checkoway, <i>Johns Hopkins University</i>	
From the Aether to the Ethernet—Attacking the Internet using Broadcast Digital Television	353
Yossef Oren and Angelos D. Keromytis, <i>Columbia University</i>	
Security Analysis of a Full-Body Scanner	369
Keaton Mowery, <i>University of California, San Diego</i> ; Eric Wustrow, <i>University of Michigan</i> ; Tom Wypych, Corey Singleton, Chris Comfort, and Eric Rescorla, <i>University of California, San Diego</i> ; Stephen Checkoway, <i>Johns Hopkins University</i> ; J. Alex Halderman, <i>University of Michigan</i> ; Hovav Shacham, <i>University of California, San Diego</i>	

(Thursday, August 21, continues on next page)

ROP: Return of the %edi

ROP is Still Dangerous: Breaking Modern Defenses385
Nicholas Carlini and David Wagner, *University of California, Berkeley*

Stitching the Gadgets: On the Ineffectiveness of Coarse-Grained Control-Flow Integrity Protection401
Lucas Davi and Ahmad-Reza Sadeghi, *Intel CRI-SC at Technische Universität Darmstadt*; Daniel Lehmann, *Technische Universität Darmstadt*; Fabian Monrose, *The University of North Carolina at Chapel Hill*

Size Does Matter: Why Using Gadget-Chain Length to Prevent Code-Reuse Attacks is Hard417
Enes Göktaş, *Vrije Universiteit Amsterdam*; Elias Athanasopoulos, *FORTH-ICS*; Michalis Polychronakis, *Columbia University*; Herbert Bos, *Vrije Universiteit Amsterdam*; Georgios Portokalidis, *Stevens Institute of Technology*

Oxymoron: Making Fine-Grained Memory Randomization Practical by Allowing Code Sharing433
Michael Backes, *Saarland University and Max Planck Institute for Software Systems (MPI-SWS)*; Stefan Nürnberger, *Saarland University*

Safer Sign-Ons

Password Managers: Attacks and Defenses449
David Silver, Suman Jana, and Dan Boneh, *Stanford University*; Eric Chen and Collin Jackson, *Carnegie Mellon University*

The Emperor's New Password Manager: Security Analysis of Web-based Password Managers465
Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song, *University of California, Berkeley*

SpanDex: Secure Password Tracking for Android481
Landon P. Cox, Peter Gilbert, Geoffrey Lawler, Valentin Pistol, Ali Razeen, Bi Wu, and Sai Cheemalapati, *Duke University*

SSOScan: Automated Testing of Web Applications for Single Sign-On Vulnerabilities495
Yuchen Zhou and David Evans, *University of Virginia*

Tracking Targeted Attacks against Civilians and NGOs

When Governments Hack Opponents: A Look at Actors and Technology511
William R. Marczak, *University of California, Berkeley and The Citizen Lab*; John Scott-Railton, *University of California, Los Angeles, and The Citizen Lab*; Morgan Marquis-Boire, *The Citizen Lab*; Vern Paxson, *University of California, Berkeley, and International Computer Science Institute*

Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware527
Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, and Greg Wiseman, *The Citizen Lab*; Phillipa Gill, *Stony Brook University*; Ronald J. Deibert, *The Citizen Lab*

A Look at Targeted Attacks Through the Lense of an NGO543
Stevens Le Blond, Adina Uritesc, and Cédric Gilbert, *Max Planck Institute for Software Systems (MPI-SWS)*; Zheng Leong Chua and Prateek Saxena, *National University of Singapore*; Engin Kirda, *Northeastern University*

Passwords

A Large-Scale Empirical Analysis of Chinese Web Passwords559
Zhigong Li and Weili Han, *Fudan University*; Wenyan Xu, *Zhejiang University*

Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts575
Dinei Florêncio and Cormac Herley, *Microsoft Research*; Paul C. van Oorschot, *Carleton University*

Telepathwords: Preventing Weak Passwords by Reading Users' Minds591
Saranga Komanduri, Richard Shay, and Lorrie Faith Cranor, *Carnegie Mellon University*; Cormac Herley and Stuart Schechter, *Microsoft Research*

Towards Reliable Storage of 56-bit Secrets in Human Memory607
Joseph Bonneau, *Princeton University*; Stuart Schechter, *Microsoft Research*

Web Security: The Browser Strikes Back

Automatically Detecting Vulnerable Websites Before They Turn Malicious	625
Kyle Soska and Nicolas Christin, <i>Carnegie Mellon University</i>	
Hulk: Eliciting Malicious Behavior in Browser Extensions	641
Alexandros Kapravelos, <i>University of California, Santa Barbara</i> ; Chris Grier, <i>University of California, Berkeley, and International Computer Science Institute</i> ; Neha Chachra, <i>University of California, San Diego</i> ; Christopher Kruegel and Giovanni Vigna, <i>University of California, Santa Barbara</i> ; Vern Paxson, <i>University of California, Berkeley, and International Computer Science Institute</i>	
Precise Client-side Protection against DOM-based Cross-Site Scripting	655
Ben Stock, <i>University of Erlangen-Nuremberg</i> ; Sebastian Lekies, Tobias Mueller, Patrick Spiegel, and Martin Johns, <i>SAP AG</i>	
On the Effective Prevention of TLS Man-in-the-Middle Attacks in Web Applications	671
Nikolaos Karapanos and Srdjan Capkun, <i>ETH Zürich</i>	

Friday, August 22, 2014

Side Channels

Scheduler-based Defenses against Cross-VM Side-channels	687
Venkatanathan Varadarajan, Thomas Ristenpart, and Michael Swift, <i>University of Wisconsin—Madison</i>	
Preventing Cryptographic Key Leakage in Cloud Virtual Machines	703
Erman Pattuk, Murat Kantarcioglu, Zhiqiang Lin, and Huseyin Ulusoy, <i>The University of Texas at Dallas</i>	
FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack	719
Yuval Yarom and Katrina Falkner, <i>The University of Adelaide</i>	
Revisiting SSL/TLS Implementations: New Bleichenbacher Side Channels and Attacks	733
Christopher Meyer, Juraj Somorovsky, Eugen Weiss, and Jörg Schwenk, <i>Ruhr-University Bochum</i> ; Sebastian Schinzel, <i>Münster University of Applied Sciences</i> ; Erik Tews, <i>Technische Universität Darmstadt</i>	

After Coffee Break Crypto

Burst ORAM: Minimizing ORAM Response Times for Bursty Access Patterns	749
Jonathan Dautrich, <i>University of California, Riverside</i> ; Emil Stefanov, <i>University of California, Berkeley</i> ; Elaine Shi, <i>University of Maryland, College Park</i>	
TRUESET: Faster Verifiable Set Computations	765
Ahmed E. Kosba, <i>University of Maryland</i> ; Dimitrios Papadopoulos, <i>Boston University</i> ; Charalampos Papamanthou, Mahmoud F. Sayed, and Elaine Shi, <i>University of Maryland</i> ; Nikos Triandopoulos, <i>RSA Laboratories and Boston University</i>	
Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture	781
Eli Ben-Sasson, <i>Technion—Israel Institute of Technology</i> ; Alessandro Chiesa, <i>Massachusetts Institute of Technology</i> ; Eran Tromer, <i>Tel Aviv University</i> ; Madars Virza, <i>Massachusetts Institute of Technology</i>	
Faster Private Set Intersection Based on OT Extension	797
Benny Pinkas, <i>Bar-Ilan University</i> ; Thomas Schneider and Michael Zohner, <i>Technische Universität Darmstadt</i>	

Program Analysis: Attack of the Codes

Dynamic Hooks: Hiding Control Flow Changes within Non-Control Data	813
Sebastian Vogl, <i>Technische Universität München</i> ; Robert Gawlik and Behrad Garmany, <i>Ruhr-University Bochum</i> ; Thomas Kittel, Jonas Pföh, and Claudia Eckert, <i>Technische Universität München</i> ; Thorsten Holz, <i>Ruhr-University Bochum</i>	
X-Force: Force-Executing Binary Programs for Security Applications	829
Fei Peng, Zhui Deng, Xiangyu Zhang, and Dongyan Xu, <i>Purdue University</i> ; Zhiqiang Lin, <i>The University of Texas at Dallas</i> ; Zhendong Su, <i>University of California, Davis</i>	

(Friday, August 22, continues on next page)

BYTEWEIGHT: Learning to Recognize Functions in Binary Code	845
Tiffany Bao, Jonathan Burket, and Maverick Woo, <i>Carnegie Mellon University</i> ; Rafael Turner, <i>University of Chicago</i> ; David Brumley, <i>Carnegie Mellon University</i>	
Optimizing Seed Selection for Fuzzing	861
Alexandre Rebert, <i>Carnegie Mellon University and ForAllSecure</i> ; Sang Kil Cha and Thanassis Avgerinos, <i>Carnegie Mellon University</i> ; Jonathan Foote and David Warren, <i>Software Engineering Institute CERT</i> ; Gustavo Grieco, <i>Centro Internacional Franco Argentino de Ciencias de la Información y de Sistemas (CIFASIS)</i> and <i>Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)</i> ; David Brumley, <i>Carnegie Mellon University</i>	
After Lunch Break Crypto	
LibFTE: A Toolkit for Constructing Practical, Format-Abiding Encryption Schemes	877
Daniel Luchaup, <i>University of Wisconsin—Madison</i> ; Kevin P. Dyer, <i>Portland State University</i> ; Somesh Jha and Thomas Ristenpart, <i>University of Wisconsin—Madison</i> ; Thomas Shrimpton, <i>Portland State University</i>	
Ad-Hoc Secure Two-Party Computation on Mobile Devices using Hardware Tokens	893
Daniel Demmler, Thomas Schneider, and Michael Zohner, <i>Technische Universität Darmstadt</i>	
ZØ: An Optimizing Distributing Zero-Knowledge Compiler	909
Matthew Fredrikson, <i>University of Wisconsin—Madison</i> ; Benjamin Livshits, <i>Microsoft Research</i>	
SDDR: Light-Weight, Secure Mobile Encounters	925
Matthew Lentz, <i>University of Maryland</i> ; Viktor Erdélyi and Paarijaat Aditya, <i>Max Planck Institute for Software Systems (MPI-SWS)</i> ; Elaine Shi, <i>University of Maryland</i> ; Peter Druschel, <i>Max Planck Institute for Software Systems (MPI-SWS)</i> ; Bobby Bhattacharjee, <i>University of Maryland</i>	
Program Analysis: A New Hope	
Enforcing Forward-Edge Control-Flow Integrity in GCC & LLVM	941
Caroline Tice, Tom Roeder, and Peter Collingbourne, <i>Google, Inc.</i> ; Stephen Checkoway, <i>Johns Hopkins University</i> ; Úlfar Erlingsson, Luis Lozano, and Geoff Pike, <i>Google, Inc.</i>	
ret2dir: Rethinking Kernel Isolation	957
Vasileios P. Kemerlis, Michalis Polychronakis, and Angelos D. Keromytis, <i>Columbia University</i>	
JIGSAW: Protecting Resource Access by Inferring Programmer Expectations	973
Hayawardh Vijayakumar and Xinyang Ge, <i>The Pennsylvania State University</i> ; Mathias Payer, <i>University of California, Berkeley</i> ; Trent Jaeger, <i>The Pennsylvania State University</i>	
Static Detection of Second-Order Vulnerabilities in Web Applications	989
Johannes Dahse and Thorsten Holz, <i>Ruhr-University Bochum</i>	
Mobile Apps and Smart Phones	
ASM: A Programmable Interface for Extending Android Security	1005
Stephan Heuser, <i>Intel CRI-SC at Technische Universität Darmstadt</i> ; Adwait Nadkarni and William Enck, <i>North Carolina State University</i> ; Ahmad-Reza Sadeghi, <i>Technische Universität Darmstadt and Center for Advanced Security Research Darmstadt (CASED)</i>	
Brahmastra: Driving Apps to Test the Security of Third-Party Components	1021
Ravi Bhoraskar, <i>Microsoft Research and University of Washington</i> ; Seungyeop Han, <i>University of Washington</i> ; Jinseong Jeon, <i>University of Maryland, College Park</i> ; Tanzirul Azim, <i>University of California, Riverside</i> ; Shuo Chen, Jaeyeon Jung, Suman Nath, and Rui Wang, <i>Microsoft Research</i> ; David Wetherall, <i>University of Washington</i>	
Peeking into Your App without Actually Seeing it: UI State Inference and Novel Android Attacks	1037
Qi Alfred Chen, <i>University of Michigan</i> ; Zhiyun Qian, <i>NEC Laboratories America</i> ; Z. Morley Mao, <i>University of Michigan</i>	
Gyrophone: Recognizing Speech from Gyroscope Signals	1053
Yan Michalevsky and Dan Boneh, <i>Stanford University</i> ; Gabi Nakibly, <i>National Research & Simulation Center, Rafael Ltd.</i>	