IEEE Symposium on Security and Privacy

May 17-20, 2009
The Claremont Resort, Oakland, California, USA
Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy

30TH symposium

Monday, 18 May 2009

8:30–8:45 **Opening**

8:45–10:15 **Attacks and Defenses**

Wirelessly Pickpocketing a Mifare Classic Card
Flavio D. Garcia, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur (Radboud U. Nijmegen)

Plaintext Recovery Attacks Against SSH
Martin R. Albrecht, Kenneth G. Paterson, Gaven J. Watson (Royal Holloway, University of London)

Exploiting Unix File-System Races via Algorithmic Complexity Attacks
Xiang Cai, Yuwei Gui, Rob Johnson (Stony Brook)

10:30–11:30 **Information Security**

Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors
Bart Coppens (Ghent U.), Ingrid Verbauwhede (Katholieke Universiteit Leuven), Bjorn De Sutter, Koen De Bosschere (Ghent U.)

Non-Interference for a Practical DIFC-Based Operating System
Maxwell Krohn (CMU), Eran Tromer (MIT)

11:30–12:00 **30th Anniversary Event**

12:00–1:30 **Lunch**

1:30–3:00 **Malicious Code**

Native Client: A Sandbox for Portable, Untrusted x86 Native Code
Bennet Yee, David Sehr, Gregory Dardyk, Brad Chen, Robert Muth, Tavis Ormandy, Shiki Okasaka, Neha Narula, Nicholas Fullagar (Google)

Automatic Reverse Engineering of Malware Emulators
Monirul Sharif, Andrea Lanzi, Jonathon Giffin, Wenke Lee (Georgia Institute of Technology)

Prospex: Protocol Specification Extraction
Paolo Milani Comparetti, Gilbert Wondracek (TU Vienna), Christopher Kruegel (UC Santa Barbara), Engin Kirda (Institute Eurecom)

3:30–5:00 **Information Leaks**

Quantifying Information Leaks in Outbound Web Traffic
Kevin Borders (Web Tap Security, Inc.), Atul Prakash (University of Michigan)

Automatic Discovery and Quantification of Information Leaks
Michael Backes (Saarland University and Max Planck Institute for Software Systems), Boris Köpf, Andrey Rybalchenko (Max Planck Institute for Software Systems)

CLAMP: Practical Prevention of Large-Scale Data Leaks
Bryan Parno, Jonathan M. McCune, Dan Wendlandt, David G. Andersen, Adrian Perrig (CMU)

6:00–8:00 **Reception and Poster Session**

Tuesday, 19 May 2009

8:30–10:00 **Privacy**

De-anonymizing Social Networks
Arvind Narayanan, Vitaly Shmatikov (UT Austin)

Privacy Weaknesses in Biometric Sketches
Koen Simoens (KU Leuven), Pim Tuyls (Intrinsic-ID), Bart Preneel (KU Leuven)

The Mastermind Attack on Genomic Data
Michael T. Goodrich (University of California, Irvine)

10:30–12:00 **Formal Foundations**

A Logic of Secure Systems and its Application to Trusted Computing
Anupam Datta, Jason Franklin, Deepak Garg, Dilsun Kaynar (CMU)

Formally Certifying the Security of Digital Signature Schemes
Santiago Zanella-Béguelin (INRIA Sophia Antipolis Méditerranée and INRIA-Microsoft Research Joint Centre), Gilles Barthe (IMDEA Software), Benjamin Grégoire (INRIA Sophia Antipolis Méditerranée and INRIA-Microsoft Research Joint Centre), Federico Olmedo (Universidad Nacional de Rosario, Argentina)

An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols
Ralf Kuesters, Tomasz Truderung (U. of Trier)

12:00–1:30 **Lunch**

1:30–2:30 **Network Security**

Sphinx: A Compact and Provably Secure Mix Format
George Danezis (Microsoft Research), Ian Goldberg (University of Waterloo)

DSybil: Optimal Sybil-Resistance for Recommendation Systems
Haifeng Yu, Chenwei Shi (National University of Singapore), Michael Kaminsky, Phillip B. Gibbons (Intel Research Pittsburgh), Feng Xiao (National University of Singapore)

3:00–4:00 **Physical Security**

Fingerprinting Blank Paper Using Commodity Scanners
William Clarkson (Princeton), Tim Weyrich (University College London), Adam Finkelstein, Nadia Heninger, Alex Halderman, Ed Felten (Princeton)

Tempest in a Teapot: Compromising Reflections Revisited
Michael Backes (Saarland University and Max Planck Institute for Software Systems), Tongbo Chen (Max Planck Institue for Informatics), Markus Duermuth (Saarland University), Hendrik P. A. Lensch (Max Planck Institute for Informatics), Martin Welk (Saarland University)

4:15–5:30 **Short Talks**

5:45–7:00 **Business Meeting**

Wednesday, 20 May 2009

9:00–10:30 **Web Security**

Blueprint: Precise Browser-Neutral Prevention of Cross-Site Scripting Attacks
Mike Ter Louw, V.N. Venkatakrishnan (University of Illinois at Chicago)

Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments
Shuo Chen (Microsoft Research), Ziqing Mao (Purdue University), Yi-Min Wang, Ming Zhang (Microsoft Research)

Secure Content Sniffing for Web Browsers, or How to Stop Papers from Reviewing Themselves
Adam Barth (UC Berkeley), Juan Caballero (CMU and UC Berkeley), Dawn Song (UC Berkeley)

11:00–12:00 **Humans and Secrets**

It's No Secret. Measuring the Security and Reliability of Authentication via 'Secret' Questions
Stuart Schechter, A. J. Bernheim Brush (Microsoft Research), Serge Egelman (CMU)

Password Cracking Using Probabilistic Context-Free Grammars
Matt Weir, Sudhir Aggarwal, Bill Glodek, Breno de Medeiros (Florida State University)

12:00–12:15 **Symposium Closing**

1:00–5:00 **Tutorials** (registration required)

A Quick Intro to Trusted Hardware
Radu Sion (Stony Brook University)

Models and Methods for Disclosure Limitation
Johannes Gehrke (Cornell University) and Ashwin Machanavajjhala (Yahoo! Research)

Thursday, 21 May 2009

Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering
Rob Erbacher (Utah State University), Matt Bishop (UC Davis), and Sean Peisert (UC Davis)

Web 2.0 Security and Privacy 2009
Larry Koved (IBM Research), Dan S. Wallach (Rice University), and Adam Barth (UC Berkeley)

Organizing Committee

General Chair: David Du (U. of Minnesota, NSF)
Program Co-Chairs: Andrew Myers (Cornell U.), David Evans (University of Virginia)
Registration Chair: Ulf Lindqvist (SRI International)
Treasurer: David Shambroom (Intersystems Corp.)
Publications Chair: Carrie Gates (CA Labs)
Posters Chair: Cristina Nita-Rotaru (Purdue U.)
Short Talks Chair: Patrick Traynor (Georgia Tech)
Web Design Chair: Adrienne Felt (UC Berkeley)