Program

30th IEEE *Symposium on Security and Privacy*

Sunday, 17 May 2009

4-7pm **Welcome Reception**

Monday, 18 May 2009

8:30–8:45am **Opening**

8:45–10:15am **Session 1: Attacks and Defenses**
Chair: Tadayoshi Kohno (U. Washington)

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

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

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

10:30–11:30am **Session 2: Information Security**
Chair: Patrick Traynor (Georgia Tech)

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

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

11:30am–noon **Special 30th Anniversary Event**

noon–1:30 **Lunch**

1:30pm **Short Talk Abstracts Due**

1:30–3:00pm **Session 3: Malicious Code**
Chair: Úlfar Erlingsson (Reykjavik U.)

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 Tech)

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

3:30–5:00pm **Session 4: Information Leaks**
Chair: Radu Sion (Stony Brook University)

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

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

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

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

Tuesday, 19 May 2009

8:30–10:00am **Session 5: Privacy**
Chair: Kristen LeFevre (University of Michigan)

De-anonymizing Social Networks
Arvind Narayanan, Vitaly Shmatikov (University of Texas, 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 (UC Irvine)

10:30am–noon **Session 6: Formal Foundations**
Chair: Vitaly Shmatikov (University of Texas, Austin)

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), Gilles Barthe (IMDEA Software), Benjamin Grégoire (INRIA), Federico Olmedo (Universidad Nacional de Rosario, Argentina)

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

noon–1:30pm **Lunch**

1:30–2:30pm **Session 7: Network Security**
Chair: Jonathon Giffin (Georgia Tech)

Sphinx: A Compact and Provably Secure Mix Format
George Danezis (Microsoft Research), Ian Goldberg (U. 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)

3:00–4:00pm **Session 8: Physical Security**
Chair: Farinaz Koushanfar (Rice University)

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 MPI-SWS), Tongbo Chen (Max Planck Institute for Informatics), Markus Duermuth (Saarland University), Hendrik P. A. Lensch (Max Planck Institute for Informatics), Martin Welk (Saarland University)

4:15–5:30pm **Short Talks**
Chair: Patrick Traynor (Georgia Tech)

Submit short talk abstracts before 1:30pm Monday, 18 May.
See http://oakland09.cs.virginia.edu for details.

5:45–7:00pm **Business Meeting**
Open to all attendees

Wednesday, 20 May 2009

9:00–10:30am **Session 9: Web Security**
Chair: Sam King (U. Illinois, Urbana-Champaign)

Blueprint: Robust Prevention of Cross-site Scripting Attacks for Existing Browsers
Mike Ter Louw, V.N. Venkatakrishnan (U. Illinois at Chicago)

Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments
Shuo Chen (Microsoft Research), Ziqing Mao (Purdue), 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)

11:00am–noon **Session 10: Humans and Secrets**
Chair: Michael Backes (Saarland U. and MPI-SWS)

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)

noon–12:15pm **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) and Ashwin Machanavajjhala (Yahoo!)

Thursday, 21 May 2009: Workshops

Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering
Rob Erbacher (Utah State), Matt Bishop 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)

http://oakland09.cs.virginia.edu