November 9–13, 2009 Chicago, Illinois, USA



Advancing Computing as a Science & Profession



Proceedings of the 16th ACM Conference on Computer and Communications Security

Sponsored by:

## **ACM SIGSAC**

Supported by:

National Science Foundation, US Army Research Office, National Security Agency, Google, Microsoft, & IBM



Advancing Computing as a Science & Profession

### The Association for Computing Machinery 2 Penn Plaza, Suite 701 New York, New York 10121-0701

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

#### **Notice to Past Authors of ACM-Published Articles**

ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that has been previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform permissions@acm.org, stating the title of the work, the author(s), and where and when published.

ISBN: 978-1-60558-352-5

Additional copies may be ordered prepaid from:

### **ACM Order Department**

PO Box 11405 New York, NY 10286-1405

Phone: 1-800-342-6626 (US and Canada) +1-212-626-0500 (all other countries) Fax: +1-212-944-1318 E-mail: acmhelp@acm.org

**ACM Order Number** 537090

Printed in the USA

### **Foreword**

Dear colleagues,

It is our pleasure to report that this year's ACM Conference on Computer and Communications Security (CCS 2009), held on November 9 - 13, 2009 in Chicago IL, USA, continues on the tradition of excellence established in previous years.

This year we received 315 submissions (a new record for CCS), with authors from 31 countries. Each paper was reviewed by at least three program committee members. The evaluation was made on the basis of their significance, novelty, and technical quality. Sometimes we solicited the opinion of outside experts. Reviewing was double-blind, meaning that the program committee was not aware of the identities and affiliations of the author(s) of each submitted paper. After the reviews were completed, the program committee conducted a month-long online discussion for each paper. Of the papers submitted, 58 were selected for presentation at the conference, resulting in an acceptance rate of 18%.

These numbers give only one indication of the selectivity and competitiveness of the conference. More importantly, the quality of many of the papers that we could not accept was also very high; we are confident that with only a little (if any) additional work, many will be accepted and appear in other high-quality conferences. In this, we hope they will have benefited from the hard work of the excellent program committee members that we had the pleasure to work with. Every effort was made to provide informative and constructive feedback to the authors of all papers. We wish to thank the program committee for the collegiality, diligence, responsiveness and enthusiasm they exhibited throughout this grueling, but also extremely rewarding process.

We are also very grateful to all other CCS 2009 organizers and the members of the CCS Steering Committee, whose work ensured a smooth organizational process.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you find the program stimulating.

Somesh Jha

Angelos D. Keromytis
CCS 2009 Program Chair

CCS 2009 Program Chair

# **Table of Contents**

A	CM CCS 2009 Conference Organization	X
A	CM CCS 2009 Program Committee	xi
A	CM CCS 2009 Additional Reviewers	xii
A	CM CCS 2009 Sponsor & Supporters	xiv
	ession: Attacks I ssion Chair: Patrick McDaniel (The Pennsylvania State University)	
•	Attacking Cryptographic Schemes Based on "Perturbation Polynomials"	1
•	Filter-resistant Code Injection on ARM  Yves Younan, Pieter Philippaerts Frank Piessens, Wouter Joosen (Katholieke Universiteit Leuven),  Sven Lachmund, Thomas Walter (DOCOMO Euro-Laboratories)	11
•	False Data Injection Attacks Against State Estimation in Electric Power Grids	21
	ession: RFID ssion Chair: Patrick Traynor (Georgia Institute of Technology)	
•	EPC RFID Tag Security Weaknesses and Defenses:  Passport Cards, Enhanced Drivers Licenses, and Beyond  Karl Koscher (University of Washington), Ari Juels (RSA Laboratories),  Vjekoslav Brajkovic, Tadayoshi Kohno (University of Washington),	33
•	An Efficient Forward Private RFID Protocol  Côme Berbain, Olivier Billet, Jonathan Etrog, Henri Gilbert (Orange Laboratories)	43
•	RFID Privacy: Relation Between Two Notions, Minimal Condition, and Efficient Construction	54
	ession: Formal Techniques ssion Chair: Cedric Fournet (Microsoft)	
•	CoSP: A General Framework for Computational Soundness Proofs  Michael Backes (Saarland University and MPI-SWS), Dennis Hofheinz (CWI),  Dominique Unruh (Saarland University)	66
•	Reactive Noninterference  Aaron Bohannon, Benjamin C. Pierce Vilhelm Sjöberg Stephanie Weirich, Steve Zdancewic (University of Pennsylvania)	79
•	Computational Soundness for Key Exchange Protocols with Symmetric Encryption Ralf Küsters, Max Tuengerthal (University of Trier)	91
•	A Probabilistic Approach to Hybrid Role Mining	101
	ession: Applied Cryptography ssion Chair: Hovav Shacham (University of California, San Diego)	
•	Efficient Pseudorandom Functions from the Decisional Linear Assumption and Weaker Variants	112

•	Improving Privacy and Security in Multi-Authority Attribute-Based Encryption	121
•	Oblivious Transfer with Access Control  Jan Camenisch (IBM Research - Zurich),  Maria Dubovitskaya (Moscow Engineering Physics Institute (State University)),  Gregory Neven (IBM Research - Zurich)	131
	ession: Anonymization Networks ssion Chair: George Danezis (Microsoft)	
•	NISAN: Network Information Service for Anonymization Networks  Andriy Panchenko, Stefan Richter, Arne Rache (RWTH Aachen University)	141
•	Certificateless Onion Routing Dario Catalano, Dario Fiore (University of Catania), Rosario Gennaro (IBM T.J. Watson Research Center)	151
•	ShadowWalker: Peer-to-peer Anonymous Communication Using Redundant Structured Topologies Prateek Mittal, Nikita Borisov (University of Illinois at Urbana-Champaign)	161
	ession: Cloud Security ssion Chair: Tadayoshi Kohno (University of Washington)	
•	Ripley: Automatically Securing Web 2.0 Applications Through Replicated Execution K. Vikram (Cornell University), Abhishek Prateek (IIT Delhi), Benjamin Livshits (Microsoft Research)	173
•	HAIL: A High-Availability and Integrity Layer for Cloud Storage	187
•	Hey, You, Get Off of My Cloud:  Exploring Information Leakage in Third-Party Compute Clouds  Thomas Ristenpart (University of California, San Diego), Eran Tromer (Massachusetts Institute of Technology), Hovav Shacham, Stefan Savage (University of California, San Diego)	199
•	Dynamic Provable Data Possession	213
	ession: Security of Mobile Services ssion Chair: Kosta Beznosov (University of British Columbia)	
•	On Cellular Botnets:  Measuring the Impact of Malicious Devices on a Cellular Network Core Patrick Traynor (Georgia Institute of Technology), Michael Lin, Machigar Ongtang Vikhyath Rao, Trent Jaeger, Patrick McDaniel, Thomas La Porta (The Pennsylvania State University)	223
•	On Lightweight Mobile Phone Application Certification William Enck, Machigar Ongtang, Patrick McDaniel (The Pennsylvania State University)	235
•	SMILE: Encounter-Based Trust for Mobile Social Services  Justin Manweiler, Ryan Scudellari Landon P. Cox (Duke University)	246
	ession: Software Security using Behavior ssion Chair: Jon Giffin (Georgia Institute of Technology)	
•	Battle of Botcraft: Fighting Bots in Online Games with Human Observational Proofs Steven Gianvecchio, Zhenyu Wu, Mengjun Xie, Haining Wang (The College of William and Mary)	256
•	Fides: Remote Anomaly-Based Cheat Detection Using Client Emulation  Edward Kaiser, Wu-chang Feng (Portland State University), Travis Schluessler (Intel Corporation)	269
•	Behavior Based Software Theft Detection Xinran Wang, Yoon-chan Jhi, Sencun Zhu, Peng Liu (The Pennsylvania State University)	280

	ession: Systems and Networks sion Chair: Cristina Nita-Rotaru (Purdue University)	
•	The Fable of the Bees: Incentivizing Robust Revocation Decision Making in Ad Hoc Networks Steffen Reidt (University of London), Mudhakar Srivatsa (IBM T.J. Watson Research Center), Shane Balfe (University of London)	.291
•	Effective Implementation of the Cell Broadband Engine <sup>™</sup> Isolation Loader	.303
•	On Achieving Good Operating Points on an ROC Plane Using Stochastic Anomaly Score Prediction Muhammad Qasim Ali, Hassan Khan, Ali Sajjad, Syed Ali Khayam (National University of Sciences and Technology, Pakistan)	.314
	ession: Privacy sion Chair: L. Jean Camp	
•	On Non-Cooperative Location Privacy: A Game-Theoretic Analysis  Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux (Ecole Polytechnique Fédérale de Lausanne),  David C. Parkes (Harvard University)	.324
•	Privacy-Preserving Genomic Computation Through Program Specialization	.338
•	Feeling-based Location Privacy Protection for Location-based Services  Toby Xu, Ying Cai (Iowa State University)	.348
•	Multi-party Off-the-Record Messaging  Ian Goldberg (University of Waterloo), Berkant Ustaoğlu (NTT Information Sharing Platform Laboratories), Matthew D. Van Gundy, Hao Chen (University of California, Davis)	.358
	ession: Anonymization Techniques sion Chair: Sven Dietrich (Stevens Tech)	
•	The Bayesian Traffic Analysis of Mix Networks  Carmela Troncoso (IBBT-K.U.Leuven, ESAT/COSIC), George Danezis (Microsoft Research, Cambridge, UK)	.369
•	AS-awareness in Tor Path Selection  Matthew Edman (Rensselaer Polytechnic Institute), Paul Syverson (U.S. Naval Research Laboratory)	.380
•	Membership-Concealing Overlay Networks  Eugene Vasserman Rob Jansen, James Tyra, Nicholas Hopper, Yongdae Kim (University of Minnesota)	.390
	ession: Embedded and Mobile Devices sion Chair: Paul Van Ooorschot (Carleton)	
•	On the Difficulty of Software-Based Attestation of Embedded Devices	.400
•	Proximity-based Access Control for Implantable Medical Devices  Kasper Bonne Rasmussen (ETH Zurich), Claude Castelluccia (INRIA),  Thomas S. Heydt-Benjamin, Srdjan Capkun (ETH Zurich)	.410
•	XCS: Cross Channel Scripting and Its Impact on Web Applications	.420
	ession: Technique for Ensuring Software Security sion Chair: V. N. Venkatakrishnan (University of Illinois, Chicago)	
•	A Security-Preserving Compiler for Distributed Programs: From Information-Flow Policies to Cryptographic Mechanisms Cédric Fournet (Microsoft Research), Gurvan Le Guernic (MSR-INRIA Joint Centre),	.432

Tamara Rezk (INRIA Sophia Antipolis)

•	Finding Bugs in Exceptional Situations of JNI Programs	442
•	Secure Open Source Collaboration: An Empirical Study of Linus' Law	453
	ession: Designing Secure Systems ssion Chair: Radu Sion (Stony Brook)	
•	On Voting Machine Design for Verification and Testability	463
•	Secure In-VM Monitoring Using Hardware Virtualization  Monirul I. Sharif, Wenke Lee (Georgia Institute of Technology), Weidong Cui (Microsoft Research),  Andrea Lanzi (Institute Eurecom)	477
•	A Metadata Calculus for Secure Information Sharing	488
•	Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords	500
	ession: Attacks II ssion Chair: J. Alex Halderman (University of Michigan)	
•	Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps	512
•	English Shellcode  Joshua Mason, Sam Small (Johns Hopkins University), Fabian Monrose (University of North Carolina, Chapel Hill), Greg MacManus (iSIGHT Partners)	524
•	Learning Your Identity and Disease from Research Papers: Information Leaks in Genome Wide Association Study Rui Wang, Yong Fuga Li, XiaoFeng Wang, Haixu Tang, Xiaoyong Zhou (Indiana University Bloomington)	534
	ession: System Security ssion Chair: Mihai Christodorescu (IBM)	
•	Countering Kernel Rootkits with Lightweight Hook Protection  Zhi Wang, Xuxian Jiang (North Carolina State University), Weidong Cui (Microsoft Research), Peng Ning (North Carolina State University)	545
•	Mapping Kernel Objects to Enable Systematic Integrity Checking  Martim Carbone (Georgia Institute of Technology), Weidong Cui (Microsoft Research),  Long Lu, Wenke Lee (Georgia Institute of Technology), Marcus Peinado (Microsoft Research),  Xuxian Jiang (North Carolina State University)	555
•	Robust Signatures for Kernel Data Structures	566
	ession: Anonymization ssion Chair: Apu Kapadia (Indiana University)	
•	A New Cell Counter Based Attack Against Tor	578
•	Scalable Onion Routing with Torsk  Jon McLachlan (University of Minnesota), Andrew Tran (Carnegie Mellon University), Nicholas Hopper, Yongdae Kim (University of Minnesota)	590
•	Anonymous Credentials on a Standard Java Card  Patrik Bichsel, Jan Camenisch, Thomas Groß (IBM Research), Victor Shoun (New York University)	600

# Session: Malware and Bots Session Chair: Weidong Cui (Microsoft)

36	ssion Chair. Weldong Cui ( <i>Microsoft)</i>	
•	Large-Scale Malware Indexing Using Function-Call Graphs Xin Hu (University of Michigan), Tzi-cker Chiueh (Stony Brook University), Kang G. Shin (University of Michigan)	611
•	Dispatcher: Enabling Active Botnet Infiltration Using Automatic Protocol Reverse-Engineering Juan Caballero, Pongsin Poosankam (Carnegie Mellon University & University of California, Berkeley), Christian Kreibich (International Computer Science Institute), Dawn Song (University of California, Berkeley)	621
•	Your Botnet Is My Botnet: Analysis of a Botnet Takeover Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna (University of California, Santa Barbara)	635
Α	uthor Index	649

# **ACM CCS 2009 Conference Organization**

General Chair: Ehab Al-Shaer (University of North Carolina, Charlotte, USA)

**Program Chairs:** Somesh Jha (University of Wisconsin, USA)

Angelos D. Keromytis (Columbia University, USA and Symantec Research Labs Europe, France)

Tutorial Chair: Ninghui Li (Purdue University, USA)

Workshop Chair: Ting Yu (North Carolina State University, USA)

**Treasurer:** Sencun Zhu (Pennsylvania State University, USA)

**Publication Chair:** Hao Chen (University of California at Davis, USA)

**Web Chair:** Peng Liu (Pennsylvania State University, USA)

Student Travel Grant Chair: Angelos Stavrou (George Mason Institute, USA)

Poster & Demo Chairs: Nikita Borisov (University of Illinois at Urbana-Champaign, USA)

Xinming Ou (Kansas State University, USA)

**Publicity Chairs:** Christopher Kruegel (University of California at Santa Barbara, USA)

Elena Ferrari (University of Insubria, Italy)

Patrons & Industry Outreach: Peng Ning (North Carolina State University, USA)

Nasir Memon (Polytechnic Institute of NYU, USA) Gail-Joon Ahn (Arizona State University, USA)

**Local Arrangements Committee:** Yan Chen (Northwestern University, USA)

V.N. Venkatakrishnan (University of Illinois Chicago, USA)

Tricha Anjali (Illinois Institute of Technology, USA) Jean-Philippe Labruyere (DePaul University, USA)

Regional Arrangements Committee: XiaoFeng Wang (Indiana University, USA)

Cristina Nita-Rotaru (Purdue University, USA) Alex Liu (University of Michigan, USA)

Nikita Borisov (University of Illinois at Urbana-Champaign, USA)

**Steering Committee Chair:** Carl Gunter (University of Illinois at Urbana-Champaign, USA)

**Steering Committee:** Peng Ning (North Carolina State University, USA)

Pierangela Samarati (University of Milan, Italy)
Paul Syverson (Naval Research Laboratory, USA)
Gene Tsudik (University of California, Irvine, USA)

Moti Yung (Google, USA)

Rei Safavi-Naini (University of Calgary, Canada)

# **ACM CCS 2009 Program Committee**

Martín Abadi (UC Santa Cruz & Microsoft, USA)

Kostas Anagnostakis (I2R/A-STAR, Singapore)

Kosta Beznosov (U British Columbia, Canada)

Dan Boneh (Stanford University, USA)

Steve Borbash (Department of Defense, USA)

Jean Camp (Indiana University, USA)

Iliano Cervesato (Carnegie Mellon University, USA)

Mihai Christodorescu (IBM Research, USA)

Debra Cook (Telcordia, USA)

Lorrie Cranor (Carnegie Mellon University, USA)

Weidong Cui (Microsoft Research, USA)

Marc Dacier (Symantec, France)

George Danezis (Microsoft Research, UK)

Claudia Diaz (KU Leuven, Belgium)

Sven Dietrich (Stevens Institute of Technology, USA)

Wenliang Du (Syracuse University, USA)

Matt Edman (Rensselaer Polytechnic Institute, USA)

Simone Fischer-Huebner (Karlstads University, Sweden)

Cedric Fournet (Microsoft Research, UK)

Jon Giffin (Georgia Institute of Technology, USA)

Virgil Gligor (Carnegie Mellon University, USA)

Eu-Jin Goh (Stanford University, USA)

Rachel Greenstadt (Drexel University, USA)

Minaxi Gupta (Indiana University, USA)

Peter Guttman (University of Auckland, New Zealand)

J. Alex Halderman (University of Michigan,, USA)

Sotiris Ioannidis (ICS/FORTH, Greece)

Trent Jaeger (Pennsylvania State University, USA)

Farnam Jahanian (University of Michigan, USA)

Rob Johnson (Stony Brook University, USA)

Apu Kapadia (MIT Lincoln Lab, USA)

Yoshi Kohno (University of Washington, USA)

Shriram Krishnamurthi (Brown University, USA)

Wenke Lee (Georgia Institute of Technology, USA)

Brian Levine (University of Massachusetts Amherst, USA)

Ninghui Li (Purdue University, USA)

Patrick McDaniel (Pennsylvania State University, USA)

Cathy Meadows (Naval Research Laboratory, USA)

Dave Molnar (University of California, Berkeley, USA)

Fabian Monrose (University of North Carolina, USA)

James Muir (Cloakware Corporation, Canada)

Peng Ning (North Carolina State University, USA)

Cristina Nita-Rotaru (Purdue University, USA)

Paul van Oorschot (Carleton University, Canada)

Lasse Øverlier (FFI, Norway)

Stefano Paraboschi (University of Bergamo, Italy)

Andrei Sabelfeld (Chalmers University of Technology, Sweden)

Kazue Sako (NEC, Japan)

Pierangela Samarati (Universita degli Studi di Milano, Italy)

R. Sekar (Stony Brook University, USA)

Hovav Shacham (University of California, San Diego, USA)

Umesh Shankar (Google, USA)

Shiuhpyng Shieh (National Chiao Tung University, Taiwan)

Anoop Singhal (NIST, USA)

Radu Sion (Stony Brook University, USA)

Jon Solworth (University of Chicago, USA)

Jessica Staddon (Palo Alto Research Center, USA)

Angelos Stavrou (George Mason University, USA)

Julie Thorpe (Carleton University, Canada)

Patrick Traynor (Georgia Institute of Technology, USA)

Jonathan Trostle (Johns Hopkins University, USA)

V.N. Venkatakrishnan (*University of Illinois Chicago, USA*)

Giovanni Vigna (University of California, Santa Barbara, USA)

Dan Wallach (Rice University, USA)

Susanne Wetzel (Stevens Institute of Technology, USA)

### **ACM CCS 2009 Additional Reviewers**

Sadia Afroz Tamara Denning Adam J. Lee Tsow Alex Roger Dingledine Timothy Leek Timur Alperovich Dan Dougherty Tiancheng Li Toshinori Araki William Enck Marc Liberatore Claudio Ardagna Michael Engling Feng-Hao Liu Aslan Askarov Ulfar Erlingsson An Liu Russ Atkinson Ariel Feldman Yao Liu Adam Aviv Sara Foresti Mike Ter Louw Ahmed Azab Alain Forget Daniel Luo Werner Backes Jun Furukawa Mohammad Mannan Michael Bailey Michael Gagnon Ziqing Mao Josep Balasch Virgil Gligor Leonardo Martucci Vijay Balasubramaniyan Andy Gordon Daniel Mayer Eugene Bart Dan Greene Jonathan McCune Moritz Y. Becker Gurvan Le Guernic Steve McLaughlin Sandeep Bhatkar Arjun Guha Cory McLean Arnar Birgisson Nataliya Guts Frank McSherry Prithvi Bisht Kirstie Hawkey Hamburg Mike Bruno Blanchet Hans Hedbom Kazuhiro Minami Hristo Bojinov Nadia Heninger Prateek Mittal Michael Brennan Jorge Hernandez-Herrero Ian Molloy Elie Bursztein Raquel Hill **Brett Moore** Joseph Calandrino Susan Hohenberger Sara Motiee Martim Carbone TienRuey Hsiang Ramaswamy Mouli Lorenzo Cavallaro FuHau Hsu Thomas Moyer Hong Chen Vincent Hu Tom Moyer Sonia Chiasson ShihKun Huang Thomas Moyer Richard Chow YuLun Huang Divya Muthukumaran Andrey Chudnov Toshiyuki Isshiki Steven Myers Stelvio Cimato Collin Jackson Tim Nelson Jeremy Clark Pooya Jaferian Nilesh Nipane Will Clarkson Karthick Jayaraman Ko Nishino Hubert Comon-Lundh Xiaoping Jia Jon Oberheide Jared Cordasco Andrew Kalafut Vassilis Pappas Ricardo Corin Hahna Kane Sarvar Patel Scott Coull Jonathan Katz Cem Paya Gabriela Cretu-Ciocarlie Dan Kiefer Bryan Payne Reza Curtmola David H King Martin Peck Reza Curtmola Pranab Kini Sean Peisert Alexei Czeskis Karl Koscher Gerardo Pelosi Huaiyu Dai Louis Kruger Roberto Perdisci Francis David Craig Labovitz Ray Perlner

Ben Pfaff Monirul Sharif Guan Wang Joe Politz Micah Sherr Qiang Wei Duminda Wijesekara Danny Joe Yoo Politz Elaine Shi Michalis Polychronakis Ji Sun Shin Ronny Windvik Scott Wolchok Vassilis Prevelakis YoungSang Shin Willard Rafnsson Charles Wright Craig Shue Matthew Wright Fahimeh Raja Jeffrey Siebert Glenn Wurster Ben Ransford Kapil Singh Sushant Sinha Eric Rescorla Guang Xiang Tamara Rezk Robin Snader Wei Xu Alfredo Rial Jacob Sorber Yunjing Xu MingHour Yang Matei Ripeanu Miroslava Sotakova Sandra Rueda Abhinav Srivastava Arkady Yerukhimovich Spiros Claudiu Eliopoulos Isamu Teranishi Joe Danny Politz Yoo Saftoiu Olivier Thonnard David Zage Alok Tongaonkar Eugen Zalinescu Amirali Salehi-Abari Thierry Sans Carmela Troncoso Stefano Zanero Prateek Saxena Stephen Tyree Bojan Zdrnja Camilo Veicco Ge Zhang Joshua Schiffman Jeffrey Seibert Hayawardh Vijayakumar Michelle Zhou Sabrina De Capitani di Yongxin Zhou Simha Sethumadhavan Emre Sezer Vimercati Zutao Zhu

# **ACM CCS 2009 Sponsor & Supporters**

Sponsor:



Supporters:











