CCS'11
Proceedings of the 18th ACM Conference on
Computer & Communications Security

Sponsored by:
ACM SIGSAC

Supported by:
US Army Research Office, National Science Foundation, Google, IBM, Microsoft Research, Nokia, Northwestern University, Pearson, Springer, & Technicolor
# Table of Contents

ACM CCS 2011 Conference Organization ............................................................................................................ xi

ACM CCS 2011 Additional Reviewers .................................................................................................................. xiii

CCS 2011 Sponsor & Supporters ........................................................................................................................ xvi

Keynote Address

- Reflections on the Evolution of Internet Threats: The Growing Imperative for a Cyber Secure Society .......................... 1
  Farnam Jahanian (National Science Foundation)

Session 1: System Security

- VIPER: Verifying the Integrity of PERipherals' Firmware .............................................................................. 3
  Yanlin Li, Jonathan M. McCune, Adrian Perrig (Carnegie Mellon University)

- Unicorn: Two-Factor Attestation for Data Security ......................................................................................... 17
  Mohammad Mannan (Concordia University), Beom Heyn Kim, Afshar Ganjali, David Lie (University of Toronto)

- Combining Control-Flow Integrity and Static Analysis for Efficient and Validated Data Sandboxing ............. 29
  Bin Zeng, Gang Tan (Lehigh University), Greg Morrisett (Harvard University)

Session 2: Composability of Cryptographic Protocols

- Composition Theorems Without Pre-Established Session Identifiers ............................................................... 41
  Ralf Küsters, Max Tuengerthal (University of Trier)

- Composability of Bellare-Rogaway Key Exchange Protocols .......................................................... 51
  Christina Brzuska, Marc Fischlin (Darmstadt University & CASED), Bogdan Warinschi, Stephen C. Williams (University of Bristol)

- A Composable Computational Soundness Notion ......................................................................................... 63
  Véronique Cottier (LORIA & CNRS), Bogdan Warinschi (University of Bristol)

Session 3: Hardware, SCADA, and Physical Security

- On the Requirements for Successful GPS Spoofing Attacks ................................................................. 75
  Nils Ole Tippenhauer, Christina Pöpper (ETH Zurich), Kasper B. Rasmussen (University of California, Irvine), Srdjan Čapkun (ETH Zurich)

- Protecting Consumer Privacy from Electric Load Monitoring ...................................................... 87
  Stephen McLaughlin, Patrick McDaniel (The Pennsylvania State University), William Aiello (University of British Columbia)

- PaperSpeckle: Microscopic Fingerprinting of Paper .............................................................................. 99
  Ashlesh Sharma, Lakshminarayanan Subramanian (New York University), Eric Brewer (University of California, Berkeley)

- On the Vulnerability of FPGA Bitstream Encryption Against Power Analysis Attacks .................. 111
  Amir Moni (Ruhr University Bochum), Alessandro Barenghi (Politecnico di Milano), Timo Kasper, Christof Paar (Ruhr University Bochum)

Session 4: Authentication and Access Control

- Text-based CAPTCHA Strengths and Weaknesses ........................................................................ 125
  Elie Bursztein, Matthieu Martin, John C. Mitchell (Stanford University)

- An Efficient User Verification System via Mouse Movements .............................................................. 139
  Nan Zheng, Aaron Paloski, Haiying Wang (The College of William and Mary)
• Policy Auditing over Incomplete Logs: Theory, Implementation and Applications .......... 151
  Deepak Garg, Limin Jia, Anupam Datta (Carnegie Mellon University)

• Automatic Error Finding in Access-Control Policies ............................................. 163
  Karthick Jayaraman (Microsoft), Vijay Ganesh (Massachusetts Institute of Technology),
  Maltesh Tripunitara (University of Waterloo), Martin Rinard (Massachusetts Institute of Technology),
  Steve Chapin (Syracuse University)

Session 5: Anonymous Communications

• Trust-based Anonymous Communication: Adversary Models and Routing Algorithms .... 175
  Aaron Johnson, Paul Syverson (U.S. Naval Research Laboratory),
  Roger Dingledine, Nick Mathewson (The Tor Project)

• Cirripede: Circumvention Infrastructure Using Router Redirection with Plausible Deniability.......... 187
  Amir Houmansadr, Giang T. K. Nguyen (University of Illinois at Urbana-Champaign),
  Matthew Caesar (University of California, Berkeley),
  Nikita Borisov (University of Illinois at Urbana-Champaign)

• Forensic Investigation of the OneSwarm Anonymous Filesharing System ..................... 201
  Swagatika Prusty, Brian Neil Levine, Marc Liberatore (University of Massachusetts, Amherst)

  Prateek Mittal, Ahmed Khurshid, Joshua Juen, Matthew Caesar, Nikita Borisov
  (University of Illinois at Urbana-Champaign)

Session 6: Web Security

• App Isolation: Get the Security of Multiple Browsers with Just One .......................... 227
  Eric Y. Chen (Carnegie Mellon University), Jason Bau (Stanford University),
  Charles Reis, Adam Barth (Google, Inc.), Collin Jackson (Carnegie Mellon University)

• Crouching Tiger – Hidden Payload: Security Risks of Scalable Vectors Graphics ............. 239
  Mario Heiderich, Tilman Frosch, Meiko Jensen, Thorsten Holz (Ruhr-University Bochum)

• Fear the EAR: Discovering and Mitigating Execution After Redirect Vulnerabilities ........ 251
  Adam Doupe, Bryce Boe, Christopher Kruegel, Giovanni Vigna (University of California, Santa Barbara)

• Automated Black-Box Detection of Side-Channel Vulnerabilities in Web Applications ... 263
  Peter Chapman, David Evans (University of Virginia)

Session 7: Malware and Intrusion Detection

• Deobfuscation of Virtualization-Obfuscated Software ............................................. 275
  Kevin Coogan, Gen Lu, Saumya Debray (University of Arizona)

• The Power of Procrastination: Detection and Mitigation of Execution-Stalling Malicious Code .......... 285
  Clemens Kolbitsch (Vienna University of Technology), Engin Kirda (Northeastern University),
  Christopher Kruegel (University of California, Santa Barbara),

• MIDeA: A Multi-Parallel Intrusion Detection Architecture ...................................... 297
  Giorgos Vasiliadis (FORTH-ICS), Michalis Polychronakis (Columbia University),
  Sotiris Ioannidis (FORTH-ICS)

• BitShred: Feature Hashing Malware for Scalable Triage and Semantic Analysis .............. 309
  Jiyong Jang, David Brumley (Carnegie Mellon University), Shobha Venkataraman (AT&T Labs – Research)

Session 8: Formal Methods and Verification

• Trace Equivalence Decision: Negative Tests and Non-determinism ............................ 321
  Vincent Cheval, Hubert Comon-Lundh, Stéphanie Delaune (LSV, ENS Cachan & CNRS)

• Extracting and Verifying Cryptographic Models from C Protocol Code by Symbolic Execution .......... 331
  Mikhail Aizatulin (The Open University), Andrew D. Gordon (Microsoft Research),
  Jan Jürjens (TU Dortmund & Fraunhofer ISST)
• Modular Code-Based Cryptographic Verification .....................................................341
Cédric Fournet, Markulf Kohlweiss (Microsoft Research), Pierre-Yves Strub (MSR-INRIA Joint Centre)

• Information-Flow Types for Homomorphic Encryptions ........................................351
Cédric Fournet (Microsoft Research), Jérémy Planul (MSR-INRIA Joint Centre), Tamara Rezk (INRIA Sophia Antipolis-Méditerranée)

Keynote Address
• Cryptographic Primitives for Building Secure and Privacy Respecting Protocols .................................................................................................361
Jan Camenisch (IBM Research - Zurich)

Session 9: Virtual Machines and Hypervisors
Deepa Srinivasan, Zhi Wang, Xuxian Jiang (North Carolina State University), Dongyan Xu (Purdue University)

• SICE: A Hardware-Level Strongly Isolated Computing Environment for x86 Multi-Core Platforms ...............................................................375
Ahmed M. Azab, Peng Ning (North Carolina State University), Xiaolan Zhang (IBM T.J. Watson Research Center)

• AmazonIA: When Elasticity Snaps Back ...............................................................389
Sven Bugiel, Stefan Nünberger (Technische Universität Darmstadt), Thomas Pöppelmann (Fraunhofer SIT), Ahmad-Reza Sadeghi (Technische Universität Darmstadt & Fraunhofer SIT), Thomas Schneider (Technische Universität Darmstadt)

• Eliminating the Hypervisor Attack Surface for a More Secure Cloud ..................401
Jakub Szefer, Eric Keller, Ruby B. Lee, Jennifer Rexford (Princeton University)

Session 10: Applied Cryptography
• How to Break XML Encryption ..........................................................................413
Tibor Jager, Juraj Somorovsky (Ruhr-University Bochum)

• Ciphers That Securely Encipher Their Own Keys ...............................................423
Mihir Bellare (University of California, San Diego), David Cash (IBM Research), Sriram Keelveedhi (University of California, San Diego)

• Password-Protected Secret Sharing ......................................................................433
Ali Bagherzandi, Stanislaw Jarecki (University of California, Irvine), Nitesh Saxena (University of Alabama), Yanbin Lu (University of California, Irvine)

• Practical Delegation of Computation Using Multiple Servers ............................445
Ran Canetti (Tel Aviv University and Boston University), Ben Riva (Tel Aviv University), Guy N. Rothblum (Microsoft Research)

Session 11: Wild Woolly Web
• Fashion Crimes: Trending-Term Exploitation on the Web ..................................455
Tyler Moore (Wellesley College), Nektarios Leontiadis, Nicolas Christin (Carnegie Mellon University)

• SURF: Detecting and Measuring Search Poisoning ...........................................467
Long Lu (Georgia Institute of Technology), Roberto Perdisci (University of Georgia), Wenke Lee (Georgia Institute of Technology)

• Cloak and Dagger: Dynamics of Web Search Cloaking .......................................477
David Y. Wang, Stefan Savage, Geoffrey M. Voelker (University of California, San Diego)
Session 12: Cloud Computing

- Proofs of Ownership in Remote Storage Systems
  Shai Halevi (IBM T.J. Watson Research Center), Danny Harnik (IBM Haifa Research Labs), Benny Pinkas (Bar Ilan University), Alexandra Shulman-Peleg (IBM Haifa Research Labs)

- How to Tell if Your Cloud Files Are Vulnerable to Drive Crashes
  Kevin D. Bowers, Marten van Dij, Ari Juels, Alina Oprea (RSA Laboratories), Ronald L. Rivest (Massachusetts Institute of Technology)

- Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds
  Kehuan Zhang, Xiaoyong Zhou, Yangyi Chen, Xiaofeng Wang (Indiana University, Bloomington), Yaoping Ruan (IBM T.J. Watson Research Center)

Session 13: Side-channel Attacks and Defenses

- iSpy: Automatic Reconstruction of Typed Input from Compromising Reflections
  Rahul Raguram, Andrew M. White, Dibyendusekhar Goswami, Fabian Monrose, Jan-Michael Frahm (University of North Carolina at Chapel Hill)

- Televisions, Video Privacy, and Powerline Electromagnetic Interference
  Miro Enev, Sidhant Gupta, Tadayoshi Kohno, Shwetak N. Patel (University of Washington)

- (sp)iPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers
  Philip Marquardt (Massachusetts Institute of Technology), Arunabhi Verma, Henry Carter, Patrick Traynor (Georgia Institute of Technology)

- Predictive Mitigation of Timing Channels in Interactive Systems
  Danfeng Zhang, Asian Askaro, Andrew C. Myers (Cornell University)

Session 14: Securing Web Applications

- WAPTEC: Whitebox Analysis of Web Applications for Parameter Tampering Exploit Construction
  Prithvi Bisht (University of Illinois), Timothy Hinrichs (University of Chicago), Nazari Skrupsky, V. N. Venkatakrishnan (University of Illinois)

- Context-Sensitive Auto-Sanitization in Web Templating Languages Using Type Qualifiers
  Mike Samuel (Google Inc.), Prateek Saxena, Dawn Song (University of California, Berkeley)

- SCRIPTGARD: Automatic Context-Sensitive Sanitization for Large-Scale Legacy Web Applications
  Prateek Saxena (University of California, Berkeley), David Molinar, Benjamin Livshits (Microsoft Research)

- Fortifying Web-Based Applications Automatically
  Shuo Tang, Nathan Dautenhahn, Samuel T. King (University of Illinois)

Session 15: Privacy and Mobile Security

- Android Permissions Demystified
  Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner (University of California, Berkeley)

- "These Aren't the Droids You're Looking For": Retrofitting Android to Protect Data from Impurous Applications
  Peter Hornyack, Seungyeop Han (University of Washington), Jaeyeon Jung, Stuart Schechter (Microsoft Research), David Wetherall (University of Washington)

- Privacy and Accountability for Location-based Aggregate Statistics
  Raluca Ada Popa (Massachusetts Institute of Technology), Andrew J. Blumberg (University of Texas, Austin), Hari Balakrishnan (Massachusetts Institute of Technology), Frank H. Li (Massachusetts Institute of Technology)

- Auctions in Do-Not-Track Compliant Internet Advertising
  Alexey Reznichenko (MPI-SWS), Saikat Guha (Microsoft Research India), Paul Francis (MPI-SWS)
Session 16: Making Secure Computation Practical

- **Practical PIR for Electronic Commerce** ................................................................. 677
  Ryan Henry, Femi Olumofin, Ian Goldberg *(University of Waterloo)*

- **Countering GATTACA: Efficient and Secure Testing of Fully-Sequenced Human Genomes** ................................................................. 691
  Pierre Baldi, Roberta Baronio, Emiliano De Cristofaro, Paolo Gasti, Gene Tsudik *(University of California, Irvine)*

- **Automatically Optimizing Secure Computation** .................................................... 703
  Florian Kerschbaum *(SAP Research)*

- **VMCrypt - Modular Software Architecture for Scalable Secure Computation** ........... 715
  Lior Malka *(Intel & University of Maryland)*

**Author Index** ........................................................................................................ 725