

October 17–21, 2011  
Chicago, Illinois, USA



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# 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**



**Association for  
Computing Machinery**

*Advancing Computing as a Science & Profession*

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

Copyright © 2011 by the Association for Computing Machinery, Inc. (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from: Publications Dept., ACM, Inc. Fax +1 (212) 869-0481 or <permissions@acm.org>.

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 (USA).

**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: 978-1-4503-1075-8**

Additional copies may be ordered prepaid from:

**ACM Order Department**

PO Box 30777  
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)  
+1-212-626-0500 (Global)  
Fax: +1-212-944-1318  
E-mail: acmhelp@acm.org  
Hours of Operation: 8:30 am – 4:30 pm ET



Printed in the USA

# CCS 2011 General Chair's Welcome

ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery. CCS is ACM's oldest conference in security area. It brings together researchers and developers for academics, government agencies, research labs and corporate sectors from all over the world. It provides an environment to conduct intellectual discussions and exchange ideas that are instrumental in shaping the future of computer and communications security. From its inception, CCS has established itself as a high standard research conference in the area of computer and communications security. This reputation continues to grow and is reflected in high selective and prestige of the technical programs.

From 2002- 2010, the number of paper submissions increased from ~150 to ~300 submissions, and reached the record of 325 in 2010. For this year, I am proud to announce that we have a much higher new record: 429 submissions. CCS 2011 received funding support of over \$50,000 from NSF, ARL, Google, IBM, Microsoft Research, Nokia, Northwestern University, Pearson, Springer, and Technicolor. The Organizing Committee of CCS 2010 has put together an outstanding program that includes 60 papers (another record!) in 16 technical sessions, two invited talks, 7 pre- and post-conferences specialized workshops, 4 tutorials, 41 posters, and two social events.

The CCS 2011 conference would not have been possible without the genuine and tireless efforts of the entire CCS 2011 Organizing Committee. We would like to congratulate them for their professionalism and commitment. We are most grateful to the authors who submitted their work to the main conference, workshops or posters. We would also like to thank the technical program committee members, the reviewers who diligently supported the peer review process, the workshop chairs who worked hard to organize the workshops, session chairs, and everyone else for their time and dedication to put together an outstanding program, as usual. We are also extremely grateful to those who are involved in making the local arrangements, designing the website, creating the publications and promotional materials, and handling registrations. Special acknowledgements go to the Steering Committee, especially the Chair Prof. Elisa Bertino, and the staff of the ACM who supported us throughout. Last, but far from least, we would like to express our gratitude to the patrons who so generously contributed to the conference and/or workshops.

I hope that that you will enjoy staying in Chicago. Two social local events (Happy Hour and Banquet) have been arranged to provide an opportunity for you to get together with friends and colleagues. I hope that you will have a rewarding and enjoyable experience in CCS 2011.

**Yan Chen**  
*CCS 2011 General Chair*  
*Northwestern University, USA*

# CCS 2011 Program Chairs' Welcome

It is a pleasure to present to you the proceedings of this year's ACM Conference on Computer and Communications Security (CCS 2011), held October 17-21 in Chicago, Illinois, USA.

This year we received a record 429 submissions from 39 countries. Each submission was reviewed by the technical program committee of 53 experts, as well as over 280 external reviewers. The final program contains 60 full papers, representing the acceptance rate of 14%.

The single-blind review process was organised in two rounds spanning 10 weeks. It included an opportunity for the authors to respond to reviews after the first round. Author response was followed by an electronic discussion among the PC members. Many reviews were assigned to PC members dynamically to maximise scrutiny and discussion of the submissions whose inclusion in the program was most uncertain. Overall, 1366 reviews were filed, including 430 from external reviewers. Despite the unexpected increase in submissions relative to CCS 2010, 327 papers received at least 3 reviews and 158 papers received at least 4 reviews, with some receiving as many as 5 or 6 reviews. The decision to allocate fewer than 3 reviews to some papers was taken on the basis of both the qualitative feedback from the first-round reviewers and a systematic quantitative analysis of the likelihood of their acceptance given the first-round reviews.

Many papers that could not be selected for presentation contained interesting results and ideas. We hope that the reviews will help improve these papers for future re-submissions. We also worked closely with the program chairs of CCS-affiliated workshops to ensure that the authors of rejected papers had an opportunity to submit their work to those venues.

We are deeply indebted to all members of the program committee for their hard work and the graciousness with which they engaged with a much higher workload than anticipated. On average, each PC member filed 23 reviews, with some volunteering for more than 30 reviews. We would also like to thank them for their enthusiastic participation in the discussions, and the valuable feedback to authors they included into their reviews. We would also like to recognise the hard work of external reviewers on whom we relied heavily this year. Some were kind enough to review bundles of papers on a particular subject – sometimes over 3 or 4 – a level of work that merits more than a casual acknowledgement.

We are grateful to all CCS 2011 organizers and members of the CCS steering committee for smoothly dealing with all other aspects of the conference and allowing us to concentrate on selecting quality papers for the technical program. Last, but certainly not least, our thanks go to all the authors who submitted papers and all attendees. We hope that you enjoy the program, and your participation at CCS helps you advance computer security research.

**Vitaly Shmatikov**

*ACM CCS 2011 Program Chair  
The University of Texas at Austin, USA*

**George Danezis**

*ACM CCS 2011 Program Chair  
Microsoft Research, Cambridge, UK*

# Table of Contents

<b>ACM CCS 2011 Conference Organization</b> .....	xi
---	----

<b>ACM CCS 2011 Additional Reviewers</b> .....	xiii
--	------

<b>CCS 2011 Sponsor &amp; Supporters</b> .....	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 Cortier (*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 Moradi (*Ruhr University Bochum*), Alessandro Barengi (*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, Haining 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*),  
Mahesh 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*)
- **Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting** ..... 215  
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  
Mihhail 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*), Jérémie 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

- **Process Out-Grafting: An Efficient “Out-of-VM” Approach for Fine-Grained Process Execution Monitoring** ..... 363  
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 Nürnberger (*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** ..... 491  
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** ..... 501  
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** ..... 515  
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** ..... 527  
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** ..... 537  
Miro Enev, Sidhant Gupta, Tadayoshi Kohno, Shwetak N. Patel (*University of Washington*)
- **(sp)iPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers** ..... 551  
Philip Marquardt (*Massachusetts Institute of Technology*),  
Arunabh Verma, Henry Carter, Patrick Traynor (*Georgia Institute of Technology*)
- **Predictive Mitigation of Timing Channels in Interactive Systems** ..... 563  
Danfeng Zhang, Aslan Askaro, Andrew C. Myers (*Cornell University*)

## Session 14: Securing Web Applications

- **WAPTEC: Whitebox Analysis of Web Applications for Parameter Tampering Exploit Construction** ..... 575  
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** ..... 587  
Mike Samuel (*Google Inc.*), Prateek Saxena, Dawn Song (*University of California, Berkeley*)
- **SCRIPTGARD: Automatic Context-Sensitive Sanitization for Large-Scale Legacy Web Applications** ..... 601  
Prateek Saxena (*University of California, Berkeley*),  
David Molnar, Benjamin Livshits (*Microsoft Research*)
- **Fortifying Web-Based Applications Automatically** ..... 615  
Shuo Tang, Nathan Dautenhahn, Samuel T. King (*University of Illinois*)

## Session 15: Privacy and Mobile Security

- **Android Permissions Demystified** ..... 627  
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 Imperious Applications** ..... 639  
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** ..... 653  
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** ..... 667  
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*)

## Poster and Demo Session

- **Poster: Destabilizing BitTorrent's Clusters to Attack High Bandwidth Leechers** ..... 725  
Florian Adamsky (*City University London*), Hassan Khan (*SEECs, NUST*), Muttukrishnan Rajarajan (*City University London*), Syed Ali Khayam (*SEECs, NUST*), Rudolf Jäger (*THM University of Applied Sciences*)
- **Poster: A Geometric Approach for Multicast Authentication in Adversarial Channels** ..... 729  
Seyed Ali Ahmadzadeh (*EURECOM*), Gordon B. Agnew (*University of Waterloo*)
- **Demo: A Comprehensive Framework Enabling Data-Minimizing Authentication** ..... 733  
Patrik Bichsel (*EURECOM*), Franz-Stefan Preiss (*IBM Research*)
- **Demo: The Ff Hardware Prototype for Privacy-Preserving RFID Authentication** ..... 737  
Erik-Oliver Blass, Kaoutar Elkhayaoui, Refik Molva (*EURECOM*), Olivier Savry, Cédric Vérehilac (*CEA/LETI*)
- **Poster: The Quest for Security Against Privilege Escalation Attacks on Android** ..... 741  
Sven Bugiel, Lucas Davi (*Technische Universität Darmstadt*), Alexandra Dmitrienko (*Fraunhofer SIT*), Thomas Fischer (*Ruhr-Universität Bochum*), Ahmad-Reza Sadeghi (*Technische Universität Darmstadt, Fraunhofer SIT*), Bhargava Shastri (*Fraunhofer SIT*)
- **Poster: A Path-Cutting Approach to Blocking XSS Worms in Social Web Networks** ..... 745  
Yinzhao Cao (*Northwestern University*), Vinod Yegneswaran, Phillip Porras (*SRI International*), Yan Chen (*Northwestern University*)
- **Poster: Control-Flow Integrity for Smartphones** ..... 749  
Lucas Davi (*Technische Universität Darmstadt*), Alexandra Dmitrienko (*Fraunhofer SIT*), Manuel Egele (*University of California, Santa Barbara*), Thomas Fischer, Thorsten Holz, Ralf Hund (*Ruhr-Universität Bochum*), Stefan Nürnberger (*Technische Universität Darmstadt*), Ahmad-Reza Sadeghi (*Technische Universität Darmstadt & Fraunhofer SIT*)
- **Poster: Arbitrators in the Security Infrastructure, Supporting Positive Anonymity** ..... 753  
Shlomi Dolev, Niv Gilboa, Ofer Hermoni (*Ben-Gurion University of the Negev*)
- **Poster: Attribute Based Broadcast Encryption with Permanent Revocation** ..... 757  
Shlomi Dolev, Niv Gilboa (*Ben-Gurion University of the Negev*), Marina Kopeetsky (*Sami-Shamoon College of Engineering*)
- **Poster: SMURFEN: A Rule Sharing Collaborative Intrusion Detection Network** ..... 761  
Carol Fung (*University of Waterloo*), Quanyan Zhu (*University of Illinois at Urbana-Champaign*), Raouf Boutaba (*University of Waterloo*), Tamer Başar (*University of Illinois at Urbana-Champaign*)
- **Poster: Applying Unsupervised Context-Based Analysis for Detecting Unauthorized Data Disclosure** ..... 765  
Ma'ayan Gafny, Asaf Shabtai, Lior Rokach, Yuval Elovici (*Ben Gurion University*)
- **Poster: Online Spam Filtering in Social Networks** ..... 769  
Hongyu Gao, Yan Chen, Kathy Lee, Diana Palsetia, Alok Choudhary (*Northwestern University*)
- **Poster: On Trust Evaluation with Missing Information in Reputation Systems** ..... 773  
Xi Gong, Ting Yu (*North Carolina State University*), Adam Lee (*University of Pittsburgh*)

• <b>Poster: Collaborative Policy Administration</b> .....	777
Weili Han, Zheran Fang, Weifeng Chen ( <i>Fudan University</i> ), Wenyuan Xu ( <i>University of South Carolina</i> ), Chang Lei ( <i>Fudan University</i> )	
• <b>Poster: Using Quantified Risk and Benefit to Strengthen the Security of Information Sharing</b> .....	781
Weili Han ( <i>Fudan University &amp; Ministry of Public Security</i> ), Chenguang Shen, Yuliang Yin, Yun Gu, Chen Chen ( <i>Fudan University</i> )	
• <b>Poster: CUD: Crowdsourcing for URL Spam Detection</b> .....	785
Jun Hu ( <i>Huazhong University of Science and Technology</i> ), Hongyu Gao ( <i>Northwestern University</i> ), Zhichun Li ( <i>NEC Research Labs</i> ), Yan Chen ( <i>Northwestern University</i> )	
• <b>Poster: Diego: A Fine-Grained Access Control for Web Browsers</b> .....	789
Ashar Javed ( <i>Hamburg University of Technology</i> )	
• <b>Poster: Privacy-Preserving Profile Similarity Computation in Online Social Networks</b> .....	793
Arjan Jeckmans, Qiang Tang, Pieter Hartel ( <i>University of Twente</i> )	
• <b>Poster: Practical Embedded Remote Attestation Using Physically Unclonable Functions</b> .....	797
Ünal Kocabas ( <i>Technische Universität Darmstadt</i> ), Ahmad Reza Sadeghi ( <i>Technische Universität Darmstadt &amp; Fraunhofer SIT &amp; Ruhr-Universität Bochum</i> ), Steffen Schulz ( <i>Technische Universität Darmstadt &amp; Ruhr-Universität Bochum &amp; Macquarie University</i> ), Christian Wachsmann ( <i>Technische Universität Darmstadt</i> )	
• <b>Poster: Mimicry Attacks Against Wireless Link Signature</b> .....	801
Yao Liu, Peng Ning ( <i>North Carolina State University</i> )	
• <b>Poster: Fast, Automatic iPhone Shoulder Surfing</b> .....	805
Federico Maggi, Alberto Volpatto ( <i>Politecnico di Milano</i> ), Simone Gasparini ( <i>INRIA Grenoble - Rhone-Alpes</i> ), Giacomo Boracchi, Stefano Zanero ( <i>Politecnico di Milano</i> )	
• <b>Poster: Preliminary Analysis of Google+'s Privacy</b> .....	809
Shah Mahmood, Yvo Desmedt ( <i>University College London</i> )	
• <b>Poster: Shaping Network Topology for Privacy and Performance</b> .....	813
Nayantara Mallesh ( <i>University of Minnesota</i> ), Matthew Wright ( <i>University of Texas at Arlington</i> )	
• <b>Poster: Trans-Organizational Role-Based Access Control</b> .....	817
Ramon Francisco Mejia, Yuichi Kaji, Hiroyuki Seki ( <i>Nara Institute of Science and Technology</i> )	
• <b>Poster: Towards Attribute Based Group Key Management</b> .....	821
Mohamed Nabeel, Elisa Bertino ( <i>Purdue University</i> )	
• <b>Poster: Making the Case for Intrinsic Personal Physical Unclonable Functions (IP-PUFs)</b> .....	825
Rishab Nithyanand, Radu Sion ( <i>Stony Brook University</i> ), John Solis ( <i>Sandia National Laboratories</i> )	
• <b>Poster: uPro – A Compartmentalization Tool Supporting Fine-Grained and Flexible Security Configuration</b> .....	829
Ben Niu, Gang Tan ( <i>Lehigh University</i> )	
• <b>Poster: Recoverable Botnets: A Hybrid C&amp;C Approach</b> .....	833
Liao Peng, Cui Xiang, Li Shuhao, Liu Chao ( <i>Chinese Academy of Sciences</i> )	
• <b>Poster: An Implementation of the Fully Homomorphic Smart-Vercauteren Crypto-System</b> .....	837
Henning Perl, Michael Brenner, Matthew Smith ( <i>Leibniz Universität Hannover</i> )	
• <b>Poster: ESPOONerbac: Enforcing Security Policies in Outsourced Environments with Encrypted RBAC</b> .....	841
Muhammad Rizwan Asghar, Giovanni Russello ( <i>CREATE-NET International Research Center</i> ), Bruno Crispo ( <i>University of Trento</i> )	
• <b>Poster: Inference Attacks Against Searchable Encryption Protocols</b> .....	845
Mohammad Saiful Islam, Mehmet Kuzu, Murat Kantarcioglu ( <i>The University of Texas at Dallas</i> )	
• <b>Demo: Secure Computation in JavaScript</b> .....	849
Axel Schröpfer, Florian Kerschbaum ( <i>SAP Research</i> )	

• <b>Poster: Can It Be More Practical? Improving Mouse Dynamics Biometric Performance</b> .....	853
Chao Shen, Zhongmin Cai ( <i>Xi'an Jiaotong University</i> ), Xiaohong Guan ( <i>Xi'an Jiaotong University &amp; Tsinghua University</i> )	
• <b>Poster: Towards Detecting DMA Malware</b> .....	857
Patrick Stewin, Jean-Pierre Seifert, Collin Mulliner ( <i>Technische Universität Berlin &amp; Deutsche Telekom Laboratories</i> )	
• <b>Poster: LBMS – Load Balancing Based on Multilateral Security in Cloud</b> .....	861
Pengfei Sun, Qingni Shen, Ying Chen, Zhonghai Wu, Cong Zhang ( <i>Peking University</i> ), Anbang Ruan ( <i>Oxford University</i> ), Liang Gu ( <i>Yale University</i> )	
• <b>Poster: Protecting Information in Systems of Systems</b> .....	865
Daniel Trivellato, Nicola Zannone ( <i>Eindhoven University of Technology</i> ), Sandro Etalle ( <i>Eindhoven University of Technology &amp; University of Twente</i> )	
• <b>Poster: A Certificateless Proxy Re-Encryption Scheme for Cloud-based Data Sharing</b> .....	869
Xiaoxin Wu ( <i>Huawei Information Technology Lab</i> ), Lei Xu, Xinwen Zhang ( <i>Huawei America Research Center</i> )	
• <b>Poster: Towards Formal Verification of DIFC Policies</b> .....	873
Zhi Yang ( <i>Chinese Academy of Sciences &amp; Information Engineering University</i> ), Lihua Yin, Miyi Duan, Shuyuan Jin ( <i>Chinese Academy of Sciences</i> )	
• <b>Poster: On Quantitative Information Flow Metrics</b> .....	877
Ji Zhu ( <i>University of Illinois at Urbana-Champaign</i> ), Mudhakar Srivatsa ( <i>IBM T.J. Watson Research Center</i> )	
• <b>Poster: Temporal Attribute-Based Encryption in Clouds</b> .....	881
Yan Zhu ( <i>Peking University</i> ), Hongxin Hu, Gail-Joon Ahn ( <i>Arizona State University</i> ), Xiaorui Gong, Shimin Chen ( <i>Peking University</i> )	
<b>Author Index</b> .....	885

# ACM CCS 2011 Conference Organization

**General Chair:** Yan Chen (*Northwestern University, USA*)

**Program Co-Chairs:** George Danezis (*Microsoft Research Cambridge, UK*)  
Vitaly Shmatikov (*University of Texas at Austin, USA*)

**Workshop Co-Chairs:** Ninghui Li (*Purdue University, USA*)  
V. N. Venkatakrishnan (*University of Illinois Chicago, USA*)

**Tutorial Co-Chairs:** Gail-Joon Ahn (*Arizona State University*)  
Brent Byunghoon Kang (*George Mason University, USA*)

**Treasurer:** Bin Xiao (*Hongkong Polytechnic University, China*)

**Publication Chair:** Dongyan Xu (*Purdue University, USA*)

**Web Chair:** Zhichun Li (*NEC Laboratories America, USA*)

**Student Travel Grant Co-Chairs:** Kang Li (*University of Georgia, USA*)  
Phillip Porras (*SRI International, USA*)

**Poster and Demo Co-Chairs:** Adam Lee (*University of Pittsburgh, USA*)  
Haining Wang (*College of William and Mary, USA*)

**Publicity Co-Chairs:** Guofei Gu (*Texas A&M University, USA*)  
Carlos Becker Westphall (*Federal University of Santa Catarina, Brazil*)

**Patron Co-Chairs:** Bei-Tseng Chu (*University of North Carolina Charlotte, USA*)  
Yong Guan (*Iowa State University, USA*)

**Local Arrangements Chair:** Xiaofeng Wang (*Indiana University at Bloomington, USA*)

**Local Arrangements Committee:** Kui Ren (*Illinois Institute of Technology, USA*)  
Dingbang Xu (*Governors State University, USA*)

**Steering Committee Chair:** Elisa Bertino (*Purdue University, USA*)

**Steering Committee:** Carl Landwehr (*University of Maryland, USA*)  
John Mitchell (*Stanford University, USA*)  
Peng Ning (*North Carolina State University, USA*)  
Rei Safavi-Naini (*University of Calgary, Canada*)  
Paul Syverson (*Naval Research Laboratory, USA*)  
Gene Tsudik (*University of California, Irvine, USA*)  
Marianne Winslett (*University of Illinois at Urbana-Champaign, USA*)  
Moti Yung (*Google, USA*)

**Program Committee:** Michael Backes (*Saarland Univ. and MPI-SWS, Germany*)  
Bruno Blanchet (*CNRS, ENS, INRIA, France*)  
Dan Boneh (*Stanford, USA*)  
Nikita Borisov (*UIUC, USA*)  
Herbert Bos (*VU, Netherlands*)

**Program Committee (continued):** Srdjan Capkun (*ETHZ, Switzerland*)  
 Avik Chaudhuri (*Adobe Advanced Technology Labs, USA*)  
 Shuo Chen (*Microsoft Research, USA*)  
 Manuel Costa (*Microsoft Research, UK*)  
 Anupam Datta (*CMU, USA*)  
 Stephanie Delaune (*CNRS and ENS-Cachan, France*)  
 Roger Dingledine (*The Tor Project, USA*)  
 Orr Dunkelman (*University of Haifa and Weizmann Institute, Israel*)  
 Ulfar Erlingsson (*Google, USA*)  
 Nick Feamster (*Georgia Tech, USA*)  
 Bryan Ford (*Yale University, USA*)  
 Cedric Fournet (*Microsoft Research, UK*)  
 Paul Francis (*MPI-SWS, Germany*)  
 Michael Freedman (*Princeton University, USA*)  
 Guofei Gu (*Texas A&M University, USA*)  
 Nicholas Hopper (*University of Minnesota, USA*)  
 Jean-Pierre Hubaux (*EPFL, Switzerland*)  
 Collin Jackson (*CMU Silicon Valley, USA*)  
 Markus Jakobsson (*Paypal, USA*)  
 Jaeyeon Jung (*Intel Labs Seattle, USA*)  
 Apu Kapadia (*Indiana University, USA*)  
 Jonathan Katz (*University of Maryland, USA*)  
 Stefan Katzenbeisser (*TU Darmstadt, Germany*)  
 Arvind Krishnamurthy (*University of Washington, USA*)  
 Christopher Kruegel (*UCSB, USA*)  
 Ralf Kuesters (*University of Trier, Germany*)  
 Ninghui Li (*Purdue University, USA*)  
 Benjamin Livshits (*Microsoft Research, USA*)  
 Heiko Mantel (*TU Darmstadt, Germany*)  
 John Mitchell (*Stanford, USA*)  
 Fabian Monrose (*UNC at Chapel Hill, USA*)  
 Steven Murdoch (*University of Cambridge, UK*)  
 David Naccache (*Ecole Normale Supérieure, France*)  
 Arvind Narayanan (*Stanford, USA*)  
 Kenny Paterson (*Royal Holloway, University of London, UK*)  
 Niels Provos (*Google, USA*)  
 Mike Reiter (*UNC at Chapel Hill, USA*)  
 Thomas Ristenpart (*University of Wisconsin, USA*)  
 Hovav Shacham (*UCSD, USA*)  
 Anil Somayaji (*Carleton University, Canada*)  
 Francois-Xavier Standaert (*UCL, Belgium, UK*)  
 Eran Tromer (*Tel Aviv University, Israel*)  
 Leendert Van Doorn (*AMD, USA*)  
 Paul Van Oorschot (*Carleton University, Canada*)  
 Bogdan Warinschi (*University of Bristol, UK*)  
 Brent Waters (*University of Texas Austin, USA*)  
 Robert Watson (*University of Cambridge, UK*)  
 Xiaowei Yang (*Duke University, USA*)  
 Haifeng Yu (*NUS, Singapore*)

# ACM CCS 2011 Additional Reviewers

Michel Abdalla	Sagar Chaki	David Freeman
Moheeb Abu Rajab	Melissa Chase	Keith Frikken
Markus Aderhold	Binbin Chen	Shailendra Fuloria
Ben Adida	Brad Chen	Sebastian Gajek
Ruj Akavipat	Eric Chen	Tal Garfinkel
Nadhem Alfardan	Vincent Cheval	Deepak Garg
Mansour Alsaleh	Csine Chevalier	Sanjam Garg
Elena Andreeva	Yannick Chevalier	Chris Gates
Baskar Anguraj	Alessandro Chiesa	Richard Gay
Jacob Appelbaum	Seung Geol Choi	Daniel Genkin
Aslan Askarov	Sherman S. M. Chow	Benedikt Gierlichs
Arthur Asuncion	Shane Clark	Peter Gilbert
Brandon Baker	Richard Clayton	Damien Giry
Lucas Ballard	Allen Clement	Mikhail Gofman
David Barrera	Iwen Coisel	Philippe Golle
Jason Bau	Scott Coull	Xun Gong
Kevin Bauer	Jason Crampton	Vipul Goyal
Josh Benaloh	Jed Crandall	Rachel Greenstadt
Emery Berger	Cas Cremers	Adam Groce
Daniel J. Bernstein	Jon Crowcroft	Thomas Gross
Igor Bilogrevic	Weidong Cui	Krishna Gummadi
Arnar Birgisson	Boris Danev	Beno Gard
Jeremiah Blocki	Anupam Das	J. Alex Halderman
Dan Bogdanov	Lucas Davi	Shai Halevi
Rainer Bohme	Emiliano De Cristofaro	Mike Hamburg
Alexandra Boldyreva	Alex Dent	William Harris
Joseph Bonneau	Alan Dunn	Carmit Hazay
Andrew Bortz	William Enck	Ryan Henry
Michael Brennan	Sarah Ereth	Cormac Herley
Christina Brzuska	Pooya Farshim	Clemens Hlauschek
Mihai Budiu	Kathi Fisler	Jeff Hodges
Philippe Bulens	Riccardo Focardi	Owen Hofmann
Elie Bursztein	Jason Franklin	Susan Hohenberger
David Cad	Pierre Francis	Thorsten Holz
David Cash	Matt Fredrikson	Amir Houmansadr

David Huang	Benoit Libert	Giang Nguyen
Yan Huang	Jay Ligatti	Kobbi Nissim
Mathias Humbert	Zhiqiang Lin	Adam O'Neill
Tomas Isdal	Zi Lin	Yossi Oren
Yuval Ishai	Debin Liu	Claudio Orlandi
Murtuza Jadliwala	Xin Liu	Xinming Ou
Sonia Jahid	Michael Locasto	Miriam Paiola
Limin Jia	Alexander Lux	Sameer Patil
Xuxian Jiang	Phil Mackenzie	Karthik Pattabiraman
Maritza Johnson	Phillip Mackenzie	Kim Pecina
Ari Juels	Mohammad Hossein Manshaei	Roberto Perdisci
Joshua Juen	Petr Marchenko	Olivier Pereira
Mike Just	Ramya Masti	Matthias Perner
Seny Kamara	Nick Mathewson	Andreas Peter
Emilia Kasper	Michael May	Duong-Hieu Phan
Aniket Kate	Jonathan Mayer	Frank Piessens
Dilsun Kaynar	Jonathan Mccune	Benny Pinkas
Michelle Kendal	John Mchugh	Jeremy Planul
Samuel King	Frank Mcsherry	David Pointcheval
Felix Klaedtke	Sebastian Meiser	Alex Popa
Francis Koeune	Filippo Menczer	Christina Popper
Markulf Kohlweiss	Kazuhiro Minami	Phil Porras
Clemens Kolbitsch	Chris Mitchell	Marcin Poturalski
Vladimir Kolesnikov	Prateek Mittal	Shi Pu
Steve Kremer	Abadelaziz Mohaisen	Elizabeth Quaglia
Shriram Krishnamurthi	Esfandiar Mohammadi	Moheeb Rajab
Srinivas Krishnan	Payman Mohassel	Kasper Rasmussen
Markus Kuhn	Andres Molina	Rob Reeder
Klaus Kursawe	David Molnar	Francesco Regazzoni
William Leddy	Hart Montgomery	Tzachy Reinman
Adam J. Lee	Tyler Moore	Tamara Rezk
Chris Lesniewski-Laas	Alexander Moshchuk	Christian Rossow
Allison Lewko	Sascha Mler	Aaron Roth
Ang Li	Shishir Nagaraja	Guy Rothblum
Peng Li	Sanjai Narain	Yannis Rouselakis
Shujun Li	Gregory Neven	Indrajit Roy

Mark Ryan	Sid Stamm	Tielei Wang
Andrei Sabelfeld	Artem Starostin	Xiaofeng Wang
Amit Sahai	Angelos Stavrou	Lei Wei
Len Sassaman	Gianluca Stringhini	Joel Weinberger
Damien Saucez	Henning Sudbrock	Emmett Witchel
Prateek Saxena	Ankur Taly	Marcin Wojcik
Stuart Schechter	Eno Thereska	Edmund Wong
Roman Schlegel	Mohammad Torabi Dashti	Matthew Wright
Thomas Schneider	Patrick Traynor	Rebecca Wright
Dominique Schroeder	Nikos Triandopoulos	Zhaoyan Xu
Jacob Schuldt	Carmela Troncoso	Jeff Yan
Eric Seidel	Tomasz Truderung	Chao Yang
Andrei Serjantov	Max Tuengerthal	Liu Yang
Monirul Sharif	Dominique Unruh	Bennet Yee
Weidong Shi	Berkant Ustaoglu	Yves Younan
Seungwon Shin	Eugene Vasserman	Murtaza Zafer
Reza Shokri	Ingrid Verbauwhede	Davide Zanetti
Arunesh Sinha	Damien Vergnaud	Jialong Zhang
Michael Sirivianos	Andreas Vogt	Xiaolan Zhang
Asia Slowinska	Marko Vukolic	Alice Zheng
Adam Smith	Qiyang Wang	Joe Zimmerman
Barbara Sprick	Rui Wang	



# CCS 2011 Sponsor & Supporters

Sponsor:



Supporters:



NORTHWESTERN  
UNIVERSITY

PEARSON

