

October 4-8, 2010
Chicago, Illinois, USA



Association for
Computing Machinery

Advancing Computing as a Science & Profession



CCS'10

Proceedings of the 17th ACM Conference on
Computer and Communications Security

Sponsored by:

ACM SIGSAC

Supported by:

**National Science Foundation, US Army Research Office, Google,
Microsoft, IBM, UNC Charlotte, and Indiana University**



**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 © 2010 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.

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: 978-1-4503-0244-9

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 11405
New York, NY 10286-1405

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

ACM Order Number 537100

Printed in the USA

CCS 2010 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- 2008, the number of paper submissions increased from ~150 to ~300 submissions and selected papers reached 51 in 2008. CCS continues to increase in 2009 and 2010 and receives a new submission record in 2010 of 325 papers. CCS 2010 received funding support of ~\$60,000 from NSF, ARL, Google, IBM Research, Microsoft Research, University of North Carolina Charlotte, Indiana University and Thompson. The Organizing Committee of CCS 2010 has put together an outstanding program that includes 15 technical sessions, an invited talk, 9 pre- and post-conferences specialized workshops, 2 short and 3 long tutorials, 44 posters and two social events. We received around 69 posters in 2010, which is over 70% increase compared with 2009.

The CCS 2010 conference would not have been possible without the genuine and tireless efforts of the entire CCS 2010 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. A special acknowledgement goes to 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 2010.

Ehab Al-Shaer

CCS 2010 General Chair

University of North Carolina, Charlotte, USA

CCS 2010 Program Chairs' Welcome

It is our pleasure to report that the tradition of excellence established in previous years will again be manifest in this year's ACM Conference on Computer and Communications Security (CCS 2010), held October 4 - 8, 2010 in Chicago IL, USA.

We received a record 325 submissions from 36 countries. Each paper was reviewed by at least three of the 54 program committee members, with 20% of submissions receiving additional reviews (in some cases, up to 6 total reviews). This effort corresponded to a massive 1029 reviews, with each PC member responsible for 18 papers on average. The evaluation was made on the basis of each submission's significance, novelty, and technical quality. After the reviews were completed, the program committee conducted a month-long online discussion for each submission. Of the papers submitted, 55 were selected for presentation at the conference (with two of these submissions merged into a single paper), representing an acceptance rate of 17%. 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 whom we had the pleasure to work with. We wish to thank the committee for the collegiality, diligence, responsiveness, and enthusiasm they exhibited throughout this grueling, but also extremely rewarding process. We also wish to thank the 223 external reviewers who provided additional input to the process.

This year, we introduced two innovations to the conference review process: review rebuttals and supplemental material. We expect both of these experiments to be repeated at least once more.

The rebuttal process proved popular with the authors, with 256 responses submitted during the designated two-day period. These helped clarify and guide the subsequent deliberation by the program committee, and we hope that they have further improved the quality of the feedback received by the authors.

In our experiment with supplemental material, authors were allowed to provide a 3-minute video (preferred) or a small number of slides with their submissions. Our goal was to improve understanding of the work by the reviewers by supplying them with an executive summary of the work in a different format. We received 27 submissions (8% of the total) with supplemental material, the large majority of which consisted of slides. The acceptance rate among these submissions was 15%, matching that of the overall conference. However, the acceptance rate for the few submissions that provided video demonstrations of their system was 42%.

We are very grateful to all other CCS 2010 organizers and the members of the CCS Steering Committee, whose efforts 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 that, once again, you will find the program stimulating.

Angelos D. Keromytis
Columbia University, USA
CCS 2010 Program Chair

Vitaly Shmatikov
University of Texas at Austin, USA
CCS 2010 Program Chair

Table of Contents

ACM CCS 2010 Conference Organization	xii
ACM CCS 2010 Additional Reviewers	xv
ACM CCS 2010 Sponsor & Supporters	xvii

Keynote Address

Session Chair: Vitaly Shmatikov

- **Adventures in Symbolic Protocol Analysis**
Jonathan K. Millen (*The MITRE Corporation*)

Session 1A: Security Analysis

Session Chair: XiaoFeng Wang (*Indiana University Bloomington*)

- **Security Analysis of India's Electronic Voting Machines**..... 1
Scott Wolchok, Eric Wustrow, J. Alex Halderman (*The University of Michigan*),
Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati (*Netindia, (P) Ltd.*),
Rop Gonggrijp
- **Dissecting One Click Frauds**..... 15
Nicolas Christin, Sally S. Yanagihara, Keisuke Kamataki (*Carnegie Mellon University*)
- **@Spam: The Underground on 140 Characters or Less**..... 27
Chris Grier (*University of California, Berkeley*), Kurt Thomas (*University of Illinois, Champaign-Urbana*),
Vern Paxson, Michael Zhang (*University of California, Berkeley*)

Session 1B: System Security

Session Chair: Angelos Stavrou (*George Mason University*)

- **HyperSentry: Enabling Stealthy In-Context Measurement of Hypervisor Integrity**..... 38
Ahmed M. Azab, Peng Ning, Zhi Wang, Xuxian Jiang (*North Carolina State University*),
Xiaolan Zhang (*IBM T.J. Watson Research Center*), Nathan C. Skalsky (*IBM Systems & Technology Group*)
- **Trail of Bytes: Efficient Support for Forensic Analysis**..... 50
Srinivas Krishnan, Kevin Z. Snow, Fabian Monroe (*University of North Carolina at Chapel Hill*)
- **Survivable Key Compromise in Software Update Systems**..... 61
Justin Samuel (*University of California, Berkeley*), Nick Mathewson (*The Tor Project*),
Justin Cappos (*University of Washington*), Roger Dingledine (*The Tor Project*)

Session 2A: Wireless and Phone Security

Session Chair: Fabian Monroe (*University of North Carolina*)

- **A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android**..... 73
David Barrera, H. Güneş Kayacik, Paul C. van Oorschot, Anil Somayaji (*Carleton University*)
- **Mobile Location Tracking in Metro Areas: Malnets and Others**..... 85
Nathaniel Husted, Steven Myers (*Indiana University, Bloomington*)
- **On Pairing Constrained Wireless Devices Based on Secrecy of Auxiliary Channels: The Case of Acoustic Eavesdropping**..... 97
Tzipora Halevi, Nitesh Saxena (*Polytechnic Institute of New York University*)
- **PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance**..... 109
Vijay A. Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael T. Hunter, Patrick Traynor
(*Georgia Institute of Technology*)

Session 2B: Applied Cryptography I

Session Chair: Nikita Borisov (*University of Illinois Urbana-Champaign*)

- **Building Efficient Fully Collusion-Resilient Traitor Tracing and Revocation Schemes**..... 121
Sanjam Garg, Abishek Kumarasubramanian, Amit Sahai (*University of California, Los Angeles*),
Brent Waters (*University of Texas*)
- **Algebraic Pseudorandom Functions with Improved Efficiency from the Augmented Cascade**..... 131
Dan Boneh, Hart W. Montgomery, Ananth Raghunathan (*Stanford University*)
- **Practical Leakage-Resilient Pseudorandom Generators** 141
Yu Yu, François-Xavier Standaert, Olivier Pereira (*Université catholique de Louvain*),
Moti Yung (*Columbia University and Google Inc.*)
- **Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions**..... 152
Sherman S. M. Chow, Yevgeniy Dodis (*New York University*),
Yannis Rouselakis, Brent Waters (*The University of Texas at Austin*)

Session 3A: Passwords and CAPTCHAs

Session Chair: George Danezis (*Microsoft Research Cambridge*)

- **Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords**..... 162
Matt Weir, Sudhir Aggarwal (*Florida State University*), Michael Collins (*Redjack LLC*),
Henry Stern (*Cisco IronPort Systems*)
- **The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis**..... 176
Yinqian Zhang, Fabian Monrose, Michael K. Reiter (*University of North Carolina at Chapel Hill*)
- **Attacks and Design of Image Recognition CAPTCHAs** 187
Bin B. Zhu (*Microsoft Research Asia*), Jeff Yan (*Newcastle University*),
Qiujie Li (*Nanjing University of Science and Technology*),
Chao Yang (*University of Science and Technology of China*), Jia Liu (*iCare Vision Tech. Co., Ltd.*),
Ning Xu (*Microsoft Research Asia*), Meng Yi (*Temple University*), Kaiwei Cai (*Beijing University*)

Session 3B: Sandboxing

Session Chair: Engin Kirda (*Eurecom*)

- **Robusta: Taming the Native Beast of the JVM**..... 201
Joseph Siefers, Gang Tan (*Lehigh University*), Greg Morrisett (*Harvard University*)
- **Retaining Sandbox Containment Despite Bugs in Privileged Memory-Safe Code** 212
Justin Cappos, Armon Dadgar, Jeff Rasley, Justin Samuel, Ivan Beschastnikh, Cosmin Barsan,
Arvind Krishnamurthy, Thomas Anderson (*University of Washington*)
- **A Control Point for Reducing Root Abuse of File-System Privileges** 224
Glenn Wurster, Paul C. van Oorschot (*Carleton University*)

Session 4A: Attacks on Secure Hardware

Session Chair: J. Alex Halderman (*University of Michigan*)

- **Modeling Attacks on Physical Unclonable Functions**..... 237
Ulrich Rührmair, Frank Sehnke, Jan Sölter (*TU München*),
Gideon Dror (*The Academic College of Tel-Aviv-Jaffa*), Srinivas Devadas (*Massachusetts Institute of Technology*),
Jürgen Schmidhuber (*TU München*)
- **Dismantling SecureMemory, CryptoMemory and CryptoRF**..... 250
Flavio D. Garcia, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur (*Radboud University Nijmegen*)
- **Attacking and Fixing PKCS#11 Security Tokens**..... 260
Matteo Bortolozzo, Matteo Centenaro, Riccardo Focardi (*Università Cà Foscari*),
Graham Steel (*LSV, INRIA & CNRS & ENS-Cachan*)

Session 4B: Information Flow

Session Chair: Emery Berger (*University of Massachusetts*)

- **An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications** 270
Dongseok Jang, Ranjit Jhala, Sorin Lerner, Hovav Shacham (*University of California, San Diego*)
- **DIFC Programs by Automatic Instrumentation** 284
William R. Harris, Somesh Jha, Thomas Reps (*University of Wisconsin, Madison*)
- **Predictive Black-Box Mitigation of Timing Channels** 297
Aslan Askarov, Danfeng Zhang, Andrew C. Myers (*Cornell University*)

Session 5A: Anonymity Networks

Session Chair: Roger Dingledine (*Tor Project*)

- **In Search of an Anonymous and Secure Lookup: Attacks on Structured Peer-to-Peer Anonymous Communication Systems** 308
Qiyang Wang, Prateek Mittal, Nikita Borisov (*University of Illinois at Urbana-Champaign*)
- **Recruiting New Tor Relays with BRAIDS** 319
Rob Jansen, Nicholas Hopper, Yongdae Kim (*University of Minnesota*)
- **An Improved Algorithm for Tor Circuit Scheduling** 329
Can Tang, Ian Goldberg (*University of Waterloo*)
- **Dissent: Accountable Anonymous Group Messaging** 340
Henry Corrigan-Gibbs, Bryan Ford (*Yale University*)

Session 5B: Formal Methods

Session Chair: Ralf Kuesters (*University of Trier*)

- **Abstraction by Set-Membership: Verifying Security Protocols and Web Services with Databases** 351
Sebastian A. Mödersheim (*Technical University of Denmark*)
- **Developing Security Protocols by Refinement** 361
Christoph Sprenger, David Basin (*ETH Zurich*)
- **Computational Indistinguishability Logic** 375
Gilles Barthe (*IMDEA Software, Spain*), Marion Daubignard (*University of Grenoble*),
Bruce Kapron (*University of Victoria*), Yassine Lakhnech (*University of Grenoble*)
- **Computationally Sound Verification of Source Code** 387
Michael Backes (*Saarland University, MPI-SWS*), Matteo Maffei, Dominique Unruh (*Saarland University*)

Session 6A: Malware

Session Chair: Thomas Reps (*University of Wisconsin Madison*)

- **AccessMiner: Using System-Centric Models for Malware Protection** 399
Andrea Lanzi, Davide Balzarotti (*Institute Eurecom*),
Christopher Kruegel (*University of California, Santa Barbara*),
Mihai Christodorescu (*IBM T.J. Watson Research Center*), Engin Kirda (*Institute Eurecom*)
- **Input Generation Via Decomposition and Re-Stitching: Finding Bugs in Malware** 413
Juan Caballero, Pongsin Poosankam (*Carnegie Mellon University & University of California, Berkeley*),
Stephen McCamant, Domagoj Babić, Dawn Song (*University of California, Berkeley*)
- **Inference and Analysis of Formal Models of Botnet Command and Control Protocols** ... 426
Chia Yuan Cho, Domagoj Babić, Eui Chul Richard Shin, Dawn Song (*University of California, Berkeley*)
- **BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections** 440
Long Lu (*Georgia Institute of Technology*), Vinod Yegneswaran, Phillip Porras (*SRI International*),
Wenke Lee (*Georgia Institute of Technology*)

Session 6B: Applied Cryptography II

Session Chair: Jonathan Trostle (*JHU APL*)

- **TASTY: Tool for Automating Secure Two-party Computations** 451
Wilko Henecka, Stefan Kögl, Ahmad-Reza Sadeghi, Thomas Schneider, Immo Wehrenberg
(*Ruhr-University Bochum*)
- **Worry-Free Encryption: Functional Encryption with Public Keys** 463
Amit Sahai, Hakan Seyalioglu (*University of California, Los Angeles*)
- **Synchronized Aggregate Signatures:
New Definitions, Constructions and Applications** 473
Jae Hyun Ahn, Matthew Green, Susan Hohenberger (*Johns Hopkins University*)
- **Secure Text Processing with Applications to Private DNA Matching** 485
Jonathan Katz, Lior Malka (*University of Maryland*)

Session 7A: Cryptographic Protocols

Session Chair: Steve Myers (*Indiana University Bloomington*)

- **On the (In)Security of IPsec in MAC-then-Encrypt Configurations** 493
Jean Paul Degabriele, Kenneth G. Paterson (*Royal Holloway, University of London*)
- **On the Soundness of Authenticate-then-Encrypt:
Formalizing the Malleability of Symmetric Encryption** 505
Ueli Maurer, Björn Tackmann (*ETH Zurich*)
- **A New Framework for Efficient Password-Based Authenticated Key Exchange** 516
Adam Groce, Jonathan Katz (*University of Maryland*)
- **Accountability: Definition and Relationship to Verifiability** 526
Ralf Küsters, Tomasz Truderung, Andreas Vogt (*University of Trier*)

Session 7B: Memory Safety and Binary Code

Session Chair: Ulfar Erlingsson (*Google*)

- **Mimimorphism: A New Approach to Binary Code Obfuscation** 536
Zhenyu Wu, Steven Gianvecchio, Mengjun Xie, Haining Wang (*The College of William and Mary*)
- **Platform-Independent Programs** 547
Sang Kil Cha, Brian Pak, David Brumley (*Carnegie Mellon University*),
Richard J. Lipton (*Georgia Institute of Technology*)
- **Return-Oriented Programming without Returns** 559
Stephen Checkoway (*University of California, San Diego*),
Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi (*Ruhr-Universität Bochum*),
Hovav Shacham (*University of California, San Diego*), Marcel Winandy (*Ruhr-Universität Bochum*)
- **DieHarder: Securing the Heap** 573
Gene Novark, Emery D. Berger (*University of Massachusetts, Amherst*)

Session 8: Web Security

Session Chair: Mihai Christodorescu (*IBM T.J. Watson Research Center*)

- **Symbolic Security Analysis of Ruby-on-Rails Web Applications** 585
Avik Chaudhuri, Jeffrey S. Foster (*University of Maryland, College Park*)
- **Sidebuster: Automated Detection and Quantification
of Side-Channel Leaks in Web Application Development** 595
Kehuan Zhang, Zhou Li, Rui Wang, XiaoFeng Wang (*Indiana University*), Shuo Chen (*Microsoft Corporation*)

- **NoTamper: Automatic Blackbox Detection of Parameter Tampering Opportunities in Web Applications** 607
Prithvi Bisht, Timothy Hinrichs, Nazari Skrupsky, Radoslaw Bobrowicz, V. N. Venkatakrishnan
(*University of Illinois at Chicago*)
- **Protecting Browsers from Cross-Origin CSS Attacks** 619
Lin-Shung Huang, Zack Weinberg (*Carnegie Mellon University*), Chris Evans (*Google*),
Collin Jackson (*Carnegie Mellon University*)

Demonstration Presentations

- **A Privacy Recommendation Wizard for Users of Social Networking Sites** 630
Lujun Fang, Heedo Kim, Kristen LeFevre, Aaron Tami (*University of Michigan*)
- **SecTag: A Multi-Policy Supported Secure Web Tag Framework** 633
Ruixuan Li, Meng Dong, Bin Liu, Jianfeng Lu, Xiaopu Ma, Kai Li
(*Huazhong University of Science and Technology*)
- **Demonstrating Cognitive Packet Network Resilience to Worm Attacks** 636
Georgia Sakellari, Erol Gelenbe (*Imperial College London*)
- **In God We Trust All Others We Monitor** 639
Patrick Stewin, Jean-Pierre Seifert (*Berlin Institute of Technology*)

Poster Presentations

- **Enhancing Resilience of Probabilistic Key Pre-Distribution Schemes for WSNs Through Hash Chaining** 642
Walid Bechkit, Abdelmadjid Bbouabdallah, Yacine Challal (*Universite de Technologie de Compiègne*)
- **TAPS: Automatically Preparing Safe SQL Queries** 645
Prithvi Bisht, A. Prasad Sistla, V. N. Venkatakrishnan (*University of Illinois at Chicago*)
- **XACML Policy Performance Evaluation Using a Flexible Load Testing Framework** 648
Bernard Butler, Brendan Jennings, Dmitri Botvich (*Waterford Institute of Technology*)
- **Protecting Portable Storage with Host Validation** 651
Kevin R. B. Butler (*University of Oregon*),
Stephen E. McLaughlin, Patrick D. McDaniel (*The Pennsylvania State University*)
- **Virtual Browser: A Web-Level Sandbox to Secure Third-Party JavaScript without Sacrificing Functionality** 654
Yinchi Cao, Zhichun Li, Vaibhav Rastogi, Yan Chen (*Northwestern University*)
- **Cardspace in the Cloud** 657
David W. Chadwick, George Inman (*University of Kent*), Paul Coxwell (*Voice Commerce Group, UK*)
- **Secure Latency Estimation with Treepile** 660
Eric Chan-Tin, Nicholas Hopper (*University of Minnesota*)
- **TEE:**
A Virtual DRTM Based Execution Environment for Secure Cloud-End Computing 663
Weiqi Dai (*Huazhong University of Science and Technology & University of Texas at San Antonio*),
Hai Jin, Deqing Zou (*Huazhong University of Science and Technology*),
Shouhuai Xu (*University of Texas at San Antonio*),
Weide Zheng, Lei Shi (*Huazhong University of Science and Technology*)
- **Laptop Theft:**
A Case Study on the Effectiveness of Security Mechanisms in Open Organizations 666
Trajce Dimkov, Wolter Pieters, Pieter Hartel (*University of Twente*)
- **Information Security for Sensors by Overwhelming Random Sequences and Permutations** 669
Shlomi Dolev, Niv Gilboa (*Ben-Gurion University*),
Marina Kopeetsky (*Sami-Shamoon College of Engineering, Israel*), Giuseppe Persiano (*Università di Salerno*),
Paul Spirakis (*University of Patras and CTI*)
- **On Verifying Stateful Dataflow Processing Services in Large-Scale Cloud Systems** 672
Juan Du, Xiaohui Gu, Ting Yu (*North Carolina State University*)

• Assessing Trust in Uncertain Information Using Bayesian Description Logic	675
Achille Fokoue, Mudhakar Srivatsa (<i>IBM T. J. Watson Research Center</i>), Robert Young (<i>Defense Science and Technology Laboratory, UK</i>)	
• Timing Attacks on PIN Input Devices	678
Denis Foo Kune, Yongdae Kim (<i>University of Minnesota</i>)	
• Detecting and Characterizing Social Spam Campaigns	681
Hongyu Gao (<i>Northwestern University</i>), Jun Hu (<i>HUST, China</i>), Christo Wilson (<i>University of California, Santa Barbara</i>), Zhichun Li, Yan Chen (<i>Northwestern University</i>), Ben Y. Zhao (<i>University of California, Santa Barbara</i>)	
• Fingerprinting Websites Using Remote Traffic Analysis	684
Xun Gong, Negar Kiyavash, Nikita Borisov (<i>University of Illinois at Urbana-Champaign</i>)	
• Efficient Sensor Node Authentication via 3GPP Mobile Communication Networks	687
Kyunuk Han, Jangseong Kim, Kwangjo Kim (<i>Korea Advanced Institute of Science and Technology</i>), Taeshik Shon (<i>Samsung Electronics, Inc., Korea</i>)	
• Rendezvous Tunnel for Anonymous Publishing	690
Ofer Hermoni, Niv Gilboa, Eyal Felstaine, Yuval Elovici, Shlomi Dolev (<i>Ben-Gurion University</i>)	
• Exploiting Social Networking Sites for Spam	693
Markus Huber, Martin Mulazzani, Edgar Weippl, Gerhard Kitzler, Sigrun Goluch (<i>SBA Research, Austria</i>)	
• An Implementation of Event and Filter Confidentiality in Pub/Sub Systems and Its Application to e-Health	696
Mihalea Ion, Giovanni Russello (<i>CREATE-NET International Research Center</i>), Bruno Crispo (<i>University of Trento</i>)	
• Privacy and Robustness for Data Aggregation in Wireless Sensor Networks	699
Marian K. Iskander, Adam J. Lee, Daniel Mossé (<i>University of Pittsburgh</i>)	
• Designing Router Scheduling Policies: A Privacy Perspective	702
Sachin Kadloor, Xun Gong, Negar Kiyavash (<i>University of Illinois at Urbana-Champaign</i>), Parv Venkatasubramaniam (<i>Lehigh University</i>)	
• CRAFT: A New Secure Congestion Control Architecture	705
Dongho Kim, Jerry T. Chiang, Yih-Chun Hu (<i>University of Illinois at Urbana-Champaign</i>), Adrian Perrig (<i>Carnegie Mellon University</i>), P. R. Kumar (<i>University of Illinois at Urbana-Champaign</i>)	
• Dialog-Based Payload Aggregation for Intrusion Detection	708
Tobias Limmer, Falko Dressler (<i>University of Erlangen</i>)	
• Protecting Location Privacy Against Inference Attacks	711
Kazuhiro Minami (<i>National Institute of Informatics, Japan</i>), Nikita Borisov (<i>University of Illinois at Urbana-Champaign</i>)	
• Designs to Account for Trust in Social Network-Based Sybil Defenses	714
Abdelaziz Mohaisen, Nicholas Hopper, Yongdae Kim (<i>University of Minnesota</i>)	
• Secure Encounter-Based Social Networks: Requirements, Challenges, and Designs	717
Abdelaziz Mohaisen (<i>University of Minnesota</i>), Eugene Y. Vasserman (<i>Kansas State University</i>), Max Schuchard, Denis Foo Kune, Yongdae Kim (<i>University of Minnesota</i>)	
• Secure Online Banking on Untrusted Computers	720
Yanlin Peng, Wenji Chen, J. Morris Chang, Yong Guan (<i>Iowa State University</i>)	
• iFriendU: Leveraging 3-Cliques to Enhance Infiltration Attacks in Online Social Networks	723
Rahul Potharaju (<i>Purdue University</i>), Bogdan Carbutar (<i>Motorola Laboratories</i>), Cristina Nita-Rotaru (<i>Purdue University</i>)	
• Losing Control of the Internet: Using the Data Plane to Attack the Control Plane	726
Max Schuchard, Abdelaziz Mohaisen, Denis Foo Kune, Nicholas Hopper, Yongdae Kim (<i>University of Minnesota</i>), Eugene Y. Vasserman (<i>Kansas State University</i>)	
• Size-Based Scheduling: A Recipe for DDOS?	729
Abdul Serwadda, Vir V. Phoha (<i>Louisiana Tech University</i>), Idris A. Rai (<i>Makerere University</i>)	

• User-Friendly Matching Protocol for Online Social Networks	732
Qiang Tang (<i>University of Twente</i>)	
• Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services	735
Guojun Wang, Qin Liu (<i>Central South University, P. R. China</i>), Jie Wu (<i>Temple University</i>)	
• Secure Dynamic Code Generation Against Spraying	738
Wei Tao, Wang Tielei, Duan Lei (<i>Peking University</i>), Luo Jing (<i>Chinese Academy of Sciences</i>)	
• Ad Hoc Broadcast Encryption	741
Qianhong Wu (<i>Universitat Rovira i Virgili & Wuhan University</i>), Bo Qin (<i>Universitat Rovira i Virgili & Xi'an University of Technology</i>), Lei Zhang, Josep Domingo-Ferrer (<i>Universitat Rovira i Virgili</i>)	
• Dynamic Window Based Multihop Authentication for WSN	744
Yao Lan, Yu Zhiliang, Zhang Tie, Gao Fuxiang (<i>Northeastern University, China</i>)	
• Spectrum Based Fraud Detection in Social Networks	747
Xiaowei Ying, Xintao Wu (<i>University of North Carolina, Charlotte</i>), Daniel Barbará (<i>George Mason University</i>)	
• A Portable TPM Based on USB Key	750
Dawei Zhang, Zhen Han (<i>Beijing Jiaotong University</i>), Guangwen Yan (<i>Beijing Watchdata System Company</i>)	
• On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption	753
Zhibin Zhou, Dijiang Huang (<i>Arizona State University</i>)	
• Efficient Provable Data Possession for Hybrid Clouds	756
Yan Zhu, Huaixi Wang, Zexing Hu (<i>Peking University</i>), Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau (<i>Arizona State University</i>)	
• A Cloud Based SIM DRM Scheme for the Mobile Internet	759
Peng Zou, Chaokun Wang, Zhang Liu, Jianmin Wang, Jia-Guang Sun (<i>Tsinghua University</i>)	
Author Index	762

ACM CCS 2010 Conference Organization

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

Program Chairs: Angelos D. Keromytis (*Columbia University, USA*)
Vitaly Shmatikov (*University of Texas at Austin, USA*)

Tutorial Chairs: Gail-Joon Ahn (*Arizona State University, USA*)
Jorge Lobo (*IBM Research, USA*)

Workshop Chairs: Ninghui Li (*Purdue University, USA*)
Ting Yu (*North Carolina State University, USA*)

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

Local Arrangements Committee: Yan Chen (Chair) (*Northwestern University, USA*)
Tricha Anjali (*Illinois Institute of Technology, USA*)
V.N. Venkatakrishnan (*University of Illinois, Chicago, USA*)

Publicity Chairs: Chris Kruegel (*University of California, Santa Barbara, USA*)
Carlos Becker Westphal (*Federal University of Santa Catarina, Brazil*)

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

Poster & Demo Chairs: Adam J. Lee (*University of Pittsburgh, USA*)
Xinming Ou (*Kansas State University, USA*)

Regional Arrangements Committee: Yong Guan (*Iowa State University, USA*)
EJ Jung (*University of Iowa, USA*)
Alex Liu (*Michigan State University, USA*)
Kui (Quinn) Ren (*Illinois Institute of Technology, USA*)

Web Chair: Kun Bai (*IBM Research, USA*)

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

Patrons & Industry Outreach: Bill Chu (*University of North Carolina at Charlotte, USA*)
XiaoFeng Wang (*Indiana University, USA*)

Steering Committee: Elisa Bertino (*Purdue 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: Ben Adida (*Harvard University, USA*)
Adam Barth (*University of California, Berkeley, USA*)
Emery Berger (*University of Massachusetts, USA*)
Bruno Blanchet (*CNRS, ENS, INRIA, France*)
Steve Borbash (*Department of Defense, USA*)
Nikita Borisov (*University of Illinois at Urbana-Champaign, USA*)
Stephen Chong (*Harvard University, USA*)
Mihai Christodorescu (*IBM Research, USA*)
Veronique Cortier (*LORIA-CNRS, France*)
Jed Crandall (*University of New Mexico, USA*)
Weidong Cui (*Microsoft Research, USA*)
Marc Dacier (*Eurecom, France*)
George Danezis (*Microsoft Research, UK*)
Roger Dingledine (*Tor Project, USA*)
Ulfar Erlingsson (*Microsoft Research, USA*)
Cédric Fournet (*Microsoft Research-INRIA, France*)
Vanessa Friaiz-Martinez (*Telefonica Research, Spain*)
Vinod Ganapathy (*Rutgers University, USA*)
Virgil Gligor (*Carnegie Mellon University, USA*)
Philippe Golle (*PARC, USA*)
Steven Gribble (*University of Washington, USA*)
Alex Halderman (*University of Michigan, USA*)
Susan Hohenberger (*Johns Hopkins University, USA*)
Trent Jaeger (*Pennsylvania State University, USA*)
Stas Jarecki (*University of California, Irvine, USA*)
Ari Juels (*RSA Laboratories, USA*)
Apu Kapadia (*Indiana University, USA*)
Engin Kirda (*Eurecom, France*)
Yoshi Kohno (*University of Washington, USA*)
Ralf Kuesters (*University of Trier, Germany*)
Michael Locasto (*George Mason University, USA*)
Tal Malkin (*Columbia University, USA*)
Patrick McDaniel (*Pennsylvania State University, USA*)
Dave Molnar (*Microsoft Research, USA*)
Fabian Monroe (*University of North Carolina, USA*)
Steven Murdoch (*University of Cambridge, UK*)
Steven Myers (*Indiana University, USA*)
David Naumann (*Stevens Institute of Technology, USA*)
Lasse Øverlier (*FFI, Norway*)
Benny Pinkas (*University of Haifa, Israel*)
Bart Preneel (*KU Leuven, Belgium*)
Tom Reps (*University of Wisconsin, USA*)
Reiner Sailer (*IBM Research, USA*)
Steve Schneider (*University of Surrey, UK*)
R. Sekar (*SUNY Stony Brook, USA*)
Anil Somayaji (*Carleton University, Canada*)

Program Committee

(continued):

Angelos Stavrou (*George Mason University, USA*)

Jonathan Trostle (*Johns Hopkins University APL, USA*)

Helen Wang (*Microsoft Research, USA*)

XiaoFeng Wang (*Indiana University, USA*)

Brent Waters (*University of Texas at Austin, USA*)

HaiFeng Yu (*NUS, Singapore*)

Yuanyuan Zhou (*University of California, San Diego, USA*)

Mary Ellen Zurko (*IBM, USA*)

ACM CCS 2010 Additional Reviewers

Michel Abdalla	Stephanie Delaune	Danesh Irani
Jae Hyun Ahn	Tamara Denning	Sonia Jahid
Timur Alperovich	Mohan Dhawan	Suman Jana
Tycho Andersen	Evan Driscoll	Quan Jia
Man Ho Au	Manuel Egele	Maritza Johnson
Ali Bagherzandi	Matthew Elder	Srikanth Kandula
Marco Balduzzi	William Enck	Rezwana Karim
Lucas Ballard	Miro Enev	Jonathan Katz
Sruthi Bandhakavi	Roya Ensafi	Stefan Katzenbeisser
Moritz Y. Becker	Junfeng Fan	Vasileios P. Kemerlis
Amos Beimel	Sebastian Faust	Darrell Kienzle
Giampaolo Bella	Nelly Fazio	Hyun Jin Kim
Josh Benaloh	Adrienne Felt	Doug Knowles
Karyn Benson	Kathi Fisler	JeongGil Ko
Lennart Beringer	Pierre-Alain Fouque	Markulf Kohlweiss
Karthikeyan Bhargavan	Jason Franklin	Clemens Kolbitsch
Leyla Bilge	Arik Friedman	Karl Koscher
Erik-Oliver Blass	Michael Gagnon	Rama Kotla
Bill Bolosky	Steven Galbraith	Hugo Krawczyk
Line Borgund	Sanjam Garg	Steve Kremer
Kevin Bowers	William Gauvin	Alptekin K�p��
Michael Brennan	Serban Gavrila	Adam J. Lee
Torgeir Broen	Roxana Geambasu	Soo Bum Lee
Sergiu Bursuc	Michael Gerbush	Corrado Leita
Amanda Burton	Steven Gianvecchio	Amit Levy
Kevin Butler	Ian Goldberg	Allison Lewko
Shakeel Butt	Xun Gong	Ninghui Li
Joseph Calandrino	Vipul Goyal	Zhou Li
Matteo Centenaro	Matthew Green	Zhuowei Li
Haowen Chan	Rachel Greenstadt	Junghee Lum
Melissa Chase	Carl Gunter	Xiaomin Liu
Avik Chaudhuri	Chuanxiong Guo	Ben Livshits
Shuo Chen	Fuchun Guo	Jay Lorch
Yangyi Chen	Brian Haberman	Roel Maes
Celine Chevalier	Helena Handschuh	Anirban Majumder
Sherman S.M. Chow	Bill Harris	Joshua Mason
Andrey Chudnov	Carmit Hazay	Annabelle McIver
Stefan Ciobaca	Nadia Heninger	Steve McLaughlin
William Clarkson	Ryan Henry	Paolo Milani Comparetti
Jared Cordasco	Cormac Herley	Kazuhiro Minami
Scott Coull	Owen Hofmann	Prateek Mittal
Gabriela Cretu-Ciocarlie	Peter Honeyman	Payman Mohassel
Charlie Curtsinger	Nicholas Hopper	Susan Molnar
Alexei Czeskis	Sotiris Ioannidis	Alex Moshchuk

Thomas Moyer
Shishir Nagaraja
Prasad Naldurg
Arvind Narayanan
Antonio Nicolosi
Guevara Noubir
Gene Novark
Adam O'Neill
Paulo Oliveira
Josh Olsen
Machigar Ongtang
Jun Pang
Vasilis Pappas
Bryan Parno
Maura Paterson
Marcus Peinado
Bo Peng
Olivier Pereira
Mike Perry
Ryan Persaud
Olgierd Pieczul
Norbert Pohlmann
Michalis Polychronakis
Donald E. Porter
Georgios Portokalidis
Pairoj Rattadilok
Maxim Raya
Mariana Raykova
Tzachy Reinman
Jennifer Rexford
Leonid Reyzin
Tamara Rezk
Alfredo Rial

Tom Ristenpart
Luis Roderio-Merino
Franziska Roesner
Stan Rosenberg
Volker Roth
Yannis Rouselakis
Indrajit Roy
Sandra Rueda
Andy Rupp
Amit Sahai
Mastooreh Salajegheh
Javier Santoyo
Joshua Schiffman
Henning Schnoor
Srinath Setty
Stefaan Seys
Hovav Shacham
Tushar Sharma
abhi shelat
Elaine Shi
Dan Simon
Michael Sirivianos
Sriram Srinivasan
Emil Stefanov
Martin Szydlowski
Torkjel Søndrol
Trond Arne Sørby
Patrick Tague
Chunyu Tang
Isamu Teranishi
Aditya Thakur
Patrick Traynor
Nikos Triandopoulos

Tomasz Truderung
Max Tuengerthal
Emma Turetsky
Mathieu Turuani
Vinod Vaikuntanathan
Ton van Deursen
Marten van Dijk
Jeffrey Vaughan
Damien Vergnaud
Hayawardh Vijayakumar
Binh Vo
Andreas Vogt
Poorvi Vora
Erez Waisbard
Michael Walfish
Rob Walters
Haining Wang
Qiyang Wang
Rui Wang
Zhaohui Wang
Susanne Wetzel
Andrew White
Daniel Wicks
Ronny Windvik
Scott Wolchok
Edmund Wong
Zhe Xia
Liu Yang
Santiago Zanella Béguelin
Stephan Zdancewic
Kehuan Zhang
Lei Zhang
Xiaoyong Zhou

ACM CCS 2010 Sponsor & Supporters

Sponsor:



Supporters:



National Science Foundation
WHERE DISCOVERIES BEGIN



U.S. Army
Research Office



Microsoft®



UNC CHARLOTTE
College of Computing and Informatics



INDIANA UNIVERSITY
SCHOOL OF INFORMATICS AND COMPUTING
Center for Security Informatics
Bloomington