

October 16–18, 2012
Raleigh, North Carolina, USA



Association for
Computing Machinery

Advancing Computing as a Science & Profession



CCS'12

The Proceedings of the 2012 ACM Conference on
Computer and Communications Security

Sponsored by:

ACM SIGSAC

Supported by:

**National Science Foundation, US Army Research Office, IBM,
North Carolina State University, Google, NQ Mobile, & IAI**



**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 © 2012 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: permissions@acm.org or Fax +1 (212) 869-0481.

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 www.copyright.com.

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: 978-1-4503-1650-7

Additional copies may be ordered prepaid from:

ACM Order No: 537120

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 2012 General Chair's Welcome

It is our great pleasure to welcome you to the 2012 ACM Conference on Computer and Communications Security (CCS). 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 its highly selective and prestigious technical program.

From 2002-2011, the number of paper submissions increase from ~150 to ~300, and reached a much higher record of 429 in 2011. For this year, we have received 426 submissions, in par with the record set in last year. CCS 2012 received funding support of over \$60,000 from ARO, NSF, the Institute for Advanced Analytics, IBM, Department of Computer Science of North Carolina State University, Google, NetQin, and IAI. The Organizing Committee of CCS 2012 has put together an outstanding program that includes 81 papers (a new record), one invited keynote talk, 6 pre- and post-conference specialized workshops, 3 tutorials, 21 posters and demos, and two social events.

The CCS 2012 conference would not have been possible without the genuine and tireless effort of the entire CCS 2012 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 and 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 not least, we would like to express our gratitude to the patrons who so generously contributed to the conference and/or workshops.

I hope that you find this program interesting and thought-provoking. Two social events have been arranged to provide an opportunity for you to get together with friends and colleagues. We wish you enjoy staying in Raleigh and have a productive and exciting week in CCS 2012!

Ting Yu

CCS 2012 General Chair

North Carolina State University, USA

CCS 2012 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 2012), held October 16–18 in Raleigh, NC, USA.

This year we received 423 submissions from 41 countries. Each submission was reviewed by a technical program committee of 61 experts as well as over 293 external reviewers. The final program contains 81 full papers, a record number for any computer security conference so far, representing an acceptance rate of 19%.

The double-blind review process was organised in two rounds; it included an opportunity for authors to respond to reviews between rounds; and was followed by a discussion amongst the PC – a process that spanned overall 10 weeks. Reviews were assigned between phases dynamically to maximise scrutiny and discussion around submissions whose inclusion in the program was most uncertain. Overall 1395 reviews were filled, including 489 from external reviewers. Overall 365 papers received at least 3 reviews and 149 papers received at least 4 reviews – some 5 or 6. The decision to allocate fewer than 3 reviews to some papers was taken on the basis of both qualitative feedback, as well as a systematic quantitative analysis of the likelihood of them being included in the program given the first round reviews.

Many papers that were not selected for presentation contained interesting results and ideas, and we hope that the authors have benefitted from reviews to improve them further and eventually present them. We have also worked closely with the Program Chairs of workshops associated with CCS to ensure that authors have an opportunity to submit their work in 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 very heavy workload. On average each filled about 23 reviews, with some volunteering for many more. We would also like to thank them for their enthusiastic participation in the discussions, and the valuable feedback they included into the final reviews. We would also like to recognise the hard work of external reviewers. Some were kind enough to review bundles of papers on a subject — sometimes over 3 or 4 – a level of work that merits more than a casual acknowledgement.

We are grateful to all CCS 2012 organizers and members of the CCS steering committee for smoothly dealing with all other aspects of the conference – allowing us to concentrate on the quality of the 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 further the field of computer security in the future.

Virgil Gligor

*ACM CCS'12 Program Chair
Carnegie Mellon University, USA*

George Danezis

*ACM CCS'12 Program Chair
Microsoft Research, UK*

Table of Contents

CCS 2012 Conference Organization	xiii
---	-------------

CCS 2012 Additional Reviewers	xvi
--	------------

CCS 2012 Sponsor & Supporters	xviii
--	--------------

Keynote Address

• On the Foundations of Trust in Networks of Humans and Computers	1
Virgil D. Gligor (<i>Carnegie Mellon University</i>)	

Session 1: Systems Security

• Fides: Selectively Hardening Software Application Components Against Kernel-Level or Process-Level Malware	2
Raoul Strackx, Frank Piessens (<i>KU Leuven</i>)	
• A Software-Hardware Architecture for Self-Protecting Data	14
Yu-Yuan Chen, Pramod A. Jamkhedkar, Ruby B. Lee (<i>Princeton University</i>)	
• Vigilare: Toward Snoop-Based Kernel Integrity Monitor	28
Hyungon Moon (<i>Seoul National University</i>), Hojoon Lee (<i>Korea Advanced Institute of Science and Technology</i>), Jihoon Lee (<i>Seoul National University</i>), Kihwan Kim (<i>Korea Advanced Institute of Science and Technology</i>), Yunheung Paek (<i>Seoul National University</i>), Brent Byunghoon Kang (<i>George Mason University</i>)	

Session 2: Transport Layer Security

• The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software	38
Martin Georgiev (<i>The University of Texas at Austin</i>), Subodh Iyengar (<i>Stanford University</i>), Suman Jana (<i>The University of Texas at Austin</i>), Rishita Anubhai, Dan Boneh (<i>Stanford University</i>), Vitaly Shmatikov (<i>The University of Texas at Austin</i>)	
• Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security	50
Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith (<i>Leibniz University Hannover</i>), Lars Baumgärtner, Bernd Freisleben (<i>Philipps University Marburg</i>)	
• A Cross-Protocol Attack on the TLS Protocol	62
Nikos Mavrogiannopoulos, Frederik Vercauteren (<i>KU Leuven</i>), Vesselin Velichkov (<i>University of Luxembourg</i>), Bart Preneel (<i>KU Leuven</i>)	

Session 3: Anonymity & Censorship

• Enhancing Tor's Performance Using Real-Time Traffic Classification	73
Masha'el AlSabah, Kevin Bauer, Ian Goldberg (<i>University of Waterloo</i>)	
• Routing Around Decoys	85
Max Schuchard, John Geddes (<i>University of Minnesota</i>), Christopher Thompson (<i>University of California, Berkeley</i>), Nicholas Hopper (<i>University of Minnesota</i>)	
• SkypeMorph: Protocol Obfuscation for Tor Bridges	97
Hooman Mohajeri Moghaddam, Baiyu Li, Mohammad Derakhshani, Ian Goldberg (<i>University of Waterloo</i>)	
• StegoTorus: A Camouflage Proxy for the Tor Anonymity System	109
Zachary Weinberg (<i>Carnegie Mellon University</i>), Jeffrey Wang (<i>Stanford University</i>), Vinod Yegneswaran, Linda Briesemeister, Steven Cheung (<i>SRI International</i>), Frank Wang, Dan Boneh (<i>Stanford University</i>)	
• CensorSpoof: Asymmetric Communication Using IP Spoofing for Censorship-Resistant Web Browsing	121
Qiyang Wang, Xun Gong, Giang T. K. Nguyen (<i>University of Illinois at Urbana-Champaign</i>), Amir Houmansadr (<i>University of Texas at Austin</i>), Nikita Borisov (<i>University of Illinois at Urbana-Champaign</i>)	

Session 4: Software Security

- **Adaptive Defenses for Commodity Software Through Virtual Application Partitioning** 133
Dimitris Geneiatakis, Georgios Portokalidis, Vasileios P. Kemerlis, Angelos D. Keromytis (*Columbia University*)
- **Leveraging “Choice” to Automate Authorization Hook Placement** 145
Divya Muthukumaran, Trent Jaeger (*The Pennsylvania State University*), Vinod Ganapathy (*Rutgers University*)
- **Binary Stirring: Self-randomizing Instruction Addresses of Legacy X86 Binary Code** 157
Richard Wartell, Vishwath Mohan, Kevin W. Hamlen, Zhiqiang Lin (*The University of Texas at Dallas*)
- **Aligot: Cryptographic Function Identification in Obfuscated Binary Programs** 109
Joan Calvet (*Université de Lorraine*), José M. Fernandez (*Ecole Polytechnique de Montréal*), Jean-Yves Marion (*Université de Lorraine*)
- **An Historical Examination of Open Source Releases and Their Vulnerabilities** 183
Nigel Edwards, Liqun Chen (*Hewlett-Packard Laboratories*)

Session 5: Mobile Security

- **Mobile Data Charging: New Attacks and Countermeasures** 195
Chunyi Peng, Chi-yu Li, Guan-Hua Tu, Songwu Lu, Lixia Zhang (*University of California, Los Angeles*)
- **New Privacy Issues in Mobile Telephony: Fix and Verification** 205
Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan (*University of Birmingham*), Nico Golde, Kevin Redon, Ravishankar Borgaonkar (*Technische Universität Berlin & Deutsche Telekom Laboratories*)
- **PScout: Analyzing the Android Permission Specification** 217
Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, David Lie (*University of Toronto*)
- **CHEX: Statically Vetting Android Apps for Component Hijacking Vulnerabilities** 229
Long Lu (*Georgia Institute of Technology*), Zhichun Li, Zhenyu Wu (*NEC Labs America, Inc.*), Wenke Lee (*Georgia Institute of Technology*), Guofei Jiang (*NEC Labs America, Inc.*)
- **Using Probabilistic Generative Models for Ranking Risks of Android Apps** 241
Hao Peng, Chris Gates, Bhaskar Sarma, Ninghui Li, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru (*Purdue University*), Ian Molloy (*IBM Research*)

Session 6: Cloud Security

- **Self-Service Cloud Computing** 253
Shakeel Butt (*Rutgers University*), H. Andrés Lagar-Cavilla (*GridCentric Inc.*), Abhinav Srivastava (*AT&T Labs-Research*), Vinod Ganapathy (*Rutgers University*)
- **Hourglass Schemes: How to Prove That Cloud Files Are Encrypted** 265
Marten van Dijk, Ari Juels, Alina Oprea (*RSA Laboratories*), Ronald L. Rivest (*Massachusetts Institute of Technology*), Emil Stefanov (*University of California, Berkeley*), Nikos Triandopoulos (*RSA Laboratories*)
- **Resource-Freeing Attacks: Improve Your Cloud Performance (at Your Neighbor’s Expense)** 281
Venkatanathan Varadarajan, Thawan Kooburat, Benjamin Farley, Thomas Ristenpart, Michael M. Swift (*University of Wisconsin-Madison*)
- **Single Round Access Privacy on Outsourced Storage** 293
Peter Williams, Radu Sion (*Stony Brook University*)
- **Cross-VM Side Channels and Their Use to Extract Private Keys** 305
Yinqian Zhang (*University of North Carolina*), Ari Juels (*RSA Laboratories*), Michael K. Reiter (*University of North Carolina*), Thomas Ristenpart (*University of Wisconsin*)

Session 7: Intrusions & Abuse

- **Kargus: A Highly-Scalable Software-Based Intrusion Detection System** 317
Muhammad Jamshed, Jihyung Lee, Sangwoo Moon, Insu Yun (*Korea Advanced Institute of Science and Technology*), Deokjin Kim, Sungryoul Lee (*NSRI*), Yung Yi, KyoungSoo Park (*Korea Advanced Institute of Science and Technology*)

- **Populated IP Addresses — Classification and Applications** 329
Chi-Yao Hong (*University of Illinois at Urbana-Champaign*), Fang Yu, Yinglian Xie (*MSR Silicon Valley*)
- **Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds**..... 341
Antonio Bianchi, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna
(*University of California, Santa Barbara*)
- **Innocent by Association: Early Recognition of Legitimate Users** 353
Yinglian Xie Fang Yu, Qifa Ke, Martin Abadi (*Microsoft Research Silicon Valley*),
Eliot Gillum, Krish Vitaldevaria, Jason Walter (*Microsoft Corporation*),
Junxian Huang, Z. Morley Mao (*University of Michigan*)

Session 8: Usability, Authentication & Trust

- **Operating System Framed in Case of Mistaken Identity: Measuring the Success of Web-Based Spoofing Attacks on OS Password-Entry Dialogs** 365
Cristian Bravo-Lillo, Lorrie Cranor, Julie Downs, Saranga Komanduri (*Carnegie Mellon University*),
Stuart Schechter (*Microsoft Research*), Manya Sleeper (*Carnegie Mellon University*)
- **The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems** 378
San-Tsai Sun, Konstantin Beznosov (*University of British Columbia*)
- **OTO: Online Trust Oracle for User-Centric Trust Establishment** 391
Tiffany Hyun-Jin Kim (*Carnegie Mellon University*), Payas Gupta (*Singapore Management University*),
Jun Han, Emmanuel Owusu, Jason Hong, Adrian Perrig (*Carnegie Mellon University*),
Debin Gao (*Singapore Management University*)
- **Strengthening User Authentication Through Opportunistic Cryptographic Identity Assertions** 404
Alexei Czeskis (*University of Washington*), Michael Dietz (*Rice University*),
Tadayoshi Kohno (*University of Washington*), Dan Wallach (*Rice University*), Dirk Balfanz (*Google*)

Session 9: Infrastructure Security & Privacy

- **Minimizing Private Data Disclosures in the Smart Grid** 415
Weining Yang, Ninghui Li, Yuan Qi, Wahbeh Qardaji (*Purdue University*),
Stephen McLaughlin, Patrick McDaniel (*Penn State University*)
- **How Secure Are Power Network Signature Based Time Stamps?** 428
Wei-Hong Chuang, Ravi Garg, Min Wu (*University of Maryland*)
- **SABOT: Specification-Based Payload Generation for Programmable Logic Controllers** 439
Stephen McLaughlin, Patrick McDaniel (*The Pennsylvania State University*)
- **GPS Software Attacks** 450
Tyler Nighswander (*Carnegie Mellon University*),
Brent Ledvina, Jonathan Diamond, Robert Brumley, David Brumley (*Carnegie Mellon University*)
- **Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems** 462
Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu (*University of South Carolina*),
Rob Miller (*Applied Communication Sciences*), Marco Gruteser (*Rugers University*)

Session 10: Applied Cryptography I

- **Machine-Generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature Schemes** 474
Joseph A. Akinyele, Matthew Green, Susan Hohenberger, Matthew W. Pagano (*Johns Hopkins University*)
- **Full Proof Cryptography: Verifiable Compilation of Efficient Zero-Knowledge Protocols** 488
José Bacelar Almeida, Manuel Barbosa (*Universidade do Minho*),
Endre Bangerter (*Bern University of Applied Sciences*), Gilles Barthe (*IMDEA Software Institute*),
Stephan Krenn (*IST Austria*), Santiago Zanella Béguelin (*Microsoft Research*)

• Publicly Verifiable Delegation of Large Polynomials and Matrix Computations, with Applications	501
Dario Fiore (<i>New York University</i>), Rosario Gennaro (<i>City College of New York</i>)	
• Secure Two-Party Computation in Sublinear (Amortized) Time	513
S. Dov Gordon (<i>Columbia University</i>), Jonathan Katz (<i>University of Maryland</i>), Vladimir Kolesnikov (<i>Alcatel-Lucent Bell Labs</i>), Fernando Krell, Tal Malkin, Mariana Raykova (<i>Columbia University</i>), Yevgeniy Vahlis (<i>AT&T Security Research Center</i>)	
• Practical Yet Universally Composable Two-Server Password-Authenticated Secret Sharing	525
Jan Camenisch (<i>IBM Research —Zurich</i>), Anna Lysyanskaya (<i>Brown University</i>), Gregory Neven (<i>IBM Research</i>)	

Book 1 Author Index	537
----------------------------------	-----

Session 11: Network Security

• Provable Security of S-BGP and other Path Vector Protocols: Model, Analysis and Extensions	541
Alexandra Boldyreva, Robert Lychev (<i>Georgia Institute of Technology</i>)	
• Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense	553
Guanhua Yan (<i>Los Alamos National Laboratory</i>), Ritchie Lee (<i>Carnegie Mellon University Silicon Valley</i>), Alex Kent, David Wolpert (<i>Los Alamos National Laboratory</i>)	
• DCast: Sustaining Collaboration in Overlay Multicast Despite Rational Collusion	567
Haifeng Yu (<i>National University of Singapore</i>), Phillip B. Gibbons (<i>Intel Labs</i>), Chenwei Shi (<i>Mozat Pte Ltd</i>)	
• PeerPress: Utilizing Enemies' P2P Strength against Them	581
Zhaoyan Xu, Lingfeng Chen, Guofei Gu (<i>Texas A&M University</i>), Christopher Kruegel (<i>University of California</i>)	
• Collaborative TCP Sequence Number Inference Attack — How to Crack Sequence Number Under a Second	593
Zhiyun Qian, Z. Morley Mao (<i>University of Michigan</i>), Yinglian Xie (<i>Microsoft Research Silicon Valley</i>)	

Session 12: Privacy

• Touching from a Distance: Website Fingerprinting Attacks and Defenses	605
Xiang Cai, Xin Cheng Zhang, Brijesh Joshi, Rob Johnson (<i>Stony Brook University</i>)	
• Protecting Location Privacy: Optimal Strategy against Localization Attacks	617
Reza Shokri (<i>École Polytechnique Fédérale de Lausanne</i>), George Theodorakopoulos (<i>Cardiff University</i>), Carmela Troncoso (<i>K.U. Leuven</i>), Jean-Pierre Hubaux, Jean-Yves Le Boudec (<i>École Polytechnique Fédérale de Lausanne</i>)	
• Deanonymizing Mobility Traces: Using Social Networks as a Side-Channel	628
Mudhakar Srivatsa (<i>IBM T. J. Watson Research Center</i>), Mike Hicks (<i>University of Maryland</i>)	
• Differentially Private Sequential Data Publication via Variable-Length N-Grams	638
Rui Chen (<i>Concordia University</i>), Gergely Acs, Claude Castelluccia (<i>INRIA</i>)	
• On Significance of the Least Significant Bits for Differential Privacy	650
Ilya Mironov (<i>Microsoft Research Silicon Valley</i>)	

Session 13: Advertising Security & Privacy

• Privacy-Aware Personalization for Mobile Advertising	662
Michaela Hardt (<i>Twitter Inc.</i>), Suman Nath (<i>Microsoft Research</i>)	
• Knowing Your Enemy: Understanding and Detecting Malicious Web Advertising	674
Zhou Li, Kehuan Zhang (<i>Indiana University at Bloomington</i>), Yinglian Xie, Fang Yu (<i>MSR Silicon Valley</i>), XiaoFeng Wang (<i>Indiana University at Bloomington</i>)	
• Non-Tracking Web Analytics	687
Istemi Ekin Akkus, Ruichuan Chen (<i>Max Planck Institute for Software Systems</i>), Michaela Hardt (<i>Twitter Inc.</i>), Paul Francis (<i>Max Planck Institute for Software Systems</i>), Johannes Gehrke (<i>Cornell University</i>)	

Session 14: Verification

- **Computational Soundness without Protocol Restrictions** 699
Michael Backes (*Saarland University and Max Planck Institute for Software Systems*), Ankit Malik (*IIT Delhi*),
Dominique Unruh (*Tartu University*)
- **Computational Verification of C Protocol Implementations by Symbolic Execution** 712
Mihail Aizatulin (*The Open University*),
Andrew D. Gordon (*Microsoft Research—Cambridge & University of Edinburgh*),
Jan Jürjens (*TU Dortmund & Fraunhofer ISST*)
- **Verified Security of Redundancy-Free Encryption from Rabin and RSA** 724
Gilles Barthe (*IMDEA Software Institute*), David Pointcheval (*École Normale Supérieure*),
Santiago Zanella Béguelin (*Microsoft Research*)

Session 15: Web Security

- **You Are What You Include: Large-Scale Evaluation of Remote JavaScript Inclusions** 736
Nick Nikiforakis (*KU Leuven*), Luca Invernizzi, Alexandros Kapravelos (*University of California, Santa Barbara*),
Steven Van Acker, Wouter Joosen (*KU Leuven*), Christopher Kruegel (*University of California, Santa Barbara*),
Frank Piessens (*KU Leuven*), Giovanni Vigna (*University of California, Santa Barbara*)
- **FlowFox: A Web Browser with Flexible and Precise Information Flow Control** 748
Willem De Groef, Dominique Devriese, Nick Nikiforakis, Frank Piessens (*KU Leuven*)
- **Scriptless Attacks — Stealing the Pie Without Touching the Sill** 760
Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk (*Ruhr-University Bochum*)

Session 16: Secure Computation

- **Secure Two-Party Computations in ANSI C** 772
Andreas Holzer (*TU Wien*), Martin Franz (*CrypTool Project*),
Stefan Katzenbeisser (*TU Darmstadt & CAsED*), Helmut Veith (*TU Wien*)
- **Foundations of Garbled Circuits** 784
Mihir Bellare (*University of California, San Diego*),
Viet Tung Hoang, Phillip Rogaway (*University of California, Davis*)
- **Salus: A System for Server-Aided Secure Function Evaluation** 797
Seny Kamara (*Microsoft Research*), Payman Mohassel (*University of Calgary*), Ben Riva (*Tel Aviv University*)

Session 17: Badware

- **Vanity, Cracks and Malware: Insights into the Anti-Copy Protection Ecosystem** 809
Markus Kammerstetter, Christian Platzer, Gilbert Wondracek (*Vienna University of Technology*)
- **Manufacturing Compromise: The Emergence of Exploit-as-a-Service** 821
Chris Grier (*University of California, Berkeley & International Computer Science Institute*),
Lucas Ballard (*Google, Inc.*), Juan Caballero (*IMDEA Software Institute*),
Neha Chachra (*University of California, San Diego*),
Christian J. Dietrich (*University of Applied Sciences Gelsenkirchen*),
Kirill Levchenko (*University of California, San Diego*), Panayiotis Mavrommatis (*Google, Inc.*),
Damon McCoy (*George Mason University*), Antonio Nappa (*IMDEA Software Institute*),
Andreas Pitsillidis (*University of California, San Diego*), Niels Provos (*Google, Inc.*),
M. Zubair Rafique (*IMDEA Software Institute*), Moheeb Abu Rajab (*Google, Inc.*),
Christian Rossow (*University of Applied Sciences Gelsenkirchen*),
Kurt Thomas (*University of California, Berkeley*),
Vern Paxson (*University of California, Berkeley & International Computer Science Institute*),
Stefan Savage, Geoffrey M. Voelker (*University of California, San Diego*)
- **Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World** 833
Leyla Bilge, Tudor Dumitras (*Symantec Research Labs*)
- **Priceless: The Role of Payments in Abuse-Advertised Goods** 845
Damon McCoy, Hitesh Dharmdasani (*George Mason University*),
Christian Kreibich (*University of California, San Diego & International Computer Science Institute*),
Geoffrey M. Voelker, Stefan Savage (*University of California, San Diego*)

Session 18: Theory

- **On the Parameterized Complexity of the Workflow Satisfiability Problem**..... 857
Jason Crampton, Gregory Gutin (*University of London*), Anders Yeo (*University of Johannesburg*)
- **Intransitive Noninterference in Nondeterministic Systems**..... 869
Kai Engelhardt, Ron van der Meyden (*The University of New South Wales*),
Chenyi Zhang (*The University of Queensland*)
- **Precise Enforcement of Progress-Sensitive Security**..... 881
Scott Moore, Aslan Askarov, Stephen Chong (*Harvard University*)
- **TreeDroid: A Tree Automaton Based Approach to Enforcing Data Processing Policies** 894
Mads Dam, Gurvan Le Guernic, Andreas Lundblad (*KTH Royal Institute of Technology*)

Session 19: Payments, Votes & Reputation

- **Double-Spending Fast Payments in Bitcoin** 906
Ghassan O. Karame (*NEC Laboratories Europe*), Elli Androulaki, Srdjan Čapkun (*ETH Zurich*)
- **Revoke and Let Live: A Secure Key Revocation API for Cryptographic Devices** 918
Véronique Cortier (*CNRS, Loria, UMR 7503*), Graham Steel (*INRIA*),
Cyrille Wiedling (*CNRS, Loria, UMR 7503*)
- **PERM: Practical Reputation-Based Blacklisting without TTPs**..... 929
Man Ho Au (*University of Wollongong*), Apu Kapadia (*Indiana University*)
- **Measuring Vote Privacy, Revisited**..... 941
David Bernhard (*University of Bristol*), Véronique Cortier (*CNRS Loria*),
Olivier Pereira (*Université Catholique de Louvain*), Bogdan Warinschi (*University of Bristol*)

Session 20: Applied Cryptography II

- **Verifiable Data Streaming**..... 953
Dominique Schröder (*Saarland University & University of Maryland*),
Heike Schröder (*Technical University of Darmstadt*)
- **Dynamic Searchable Symmetric Encryption** 965
Seny Kamara (*Microsoft Research*), Charalampos Papamanthou (*University of California, Berkeley*),
Tom Roeder (*Microsoft Research*)
- **PrivateFS: A Parallel Oblivious File System**..... 977
Peter Williams, Radu Sion, Alin Tomescu (*Stony Brook University*)

Posters & Demos

- **POSTER: Towards Measuring Warning Readability**..... 989
Marian Harbach, Sascha Fahl, Thomas Muders, Matthew Smith (*Leibniz Universität Hannover*)
- **POSTER: Context-Aware Web Security Threat Prevention** 992
Lung-Hao Lee (*National Taiwan University & National Taiwan Normal University*), Yen-Cheng Juan,
Kuei-Ching Lee, Wei-Lin Tseng, Hsin-Hsi Chen, Yuen-Hsien Tseng (*National Taiwan Normal University*)
- **POSTER: Understanding New Anonymity Networks from a User's Perspective** 995
Erik Archambault, Craig A. Shue (*Worcester Polytechnic Institute*)
- **DEMO: Demonstrating the Effectiveness of MOSES for Separation of Execution Modes**..... 998
Giovanni Russello (*University of Auckland*), Mauro Conti (*Università di Padova*), Bruno Crispo (*Università di Trento*), Earlene Fernandes (*Vrije Universiteit Amsterdam*), Yury Zhauniarovich (*Università di Trento*)
- **POSTER: Protecting Access Privacy of Cached Contents in Information Centric Networks** 1001
Abedelaziz Mohaisen (*Verisign Labs*), Xinwen Zhang (*Huawei Technologies*),
Max Schuchard (*University of Minnesota*), Haiyong Xie (*Huawei Technologies & USTC*),
Yongdae Kim (*Korea Advanced Institute of Science and Technology*)

• POSTER: Network-Based Intrusion Detection Systems Go Active!	1004
Eitan Menahem, Yuval Elovici (<i>Ben-Gurion University of the Negev</i>), Gabi Nakibly (<i>Rafael — Advanced Defense Systems Ltd.</i>)	
• POSTER: Real-Time Continuous Iris Recognition for Authentication Using an Eye Tracker	1007
Kenrick Mock, Bogdan Hoanca, Justin Weaver, Mikal Milton (<i>University of Alaska Anchorage</i>)	
• DEMO — ReasONets: A Fuzzy-Based Approach for Reasoning on Network Incidents	1010
Giuseppe Petracca, Anna Squicciarini (<i>The Pennsylvania State University</i>), William Horne (<i>Hewlett-Packard Research Labs</i>), Marco Casassa-Mont (<i>Hewlett-Packard Research Labs</i>)	
• DEMO: How Privacy Leaks from Bluetooth Mouse?	1013
Xian Pan (<i>University of Massachusetts, Lowell</i>), Zhen Ling (<i>Southeast University</i>), Aniket Pingley (<i>Intel Inc.</i>), Wei Yu (<i>Towson University</i>), Nan Zhang (<i>George Washington University</i>), Xinwen Fu (<i>University of Massachusetts, Lowell</i>)	
• POSTER: Marlin — Making It Harder to Fish for Gadgets	1016
Aditi Gupta, Sam Kerr (<i>Purdue University</i>), Michael S. Kirkpatrick (<i>James Madison University</i>), Elisa Bertino (<i>Purdue University</i>)	
• POSTER: Advanced Triple-Channel Botnets: Model and Implementation	1019
Cui Xiang, Fang Binxing, Liao Peng, Liu Chaoge (<i>Chinese Academy of Sciences</i>)	
• DEMO: Demonstrating a Lightweight Data Provenance for Sensor Networks	1022
Bilal Shebaro, Salmin Sultana, Shakthidhar Reddy Gopavaram, Elisa Bertino (<i>Purdue University</i>)	
• POSTER: Location Privacy Leaking from Spectrum Utilization Information in Database-Driven Cognitive Radio Network	1025
Zhaoyu Gao, Haojin Zhu (<i>Shanghai Jiao Tong University</i>), Yao Liu (<i>University of South Florida</i>), Muyuan Li, Zhenfu Cao (<i>Shanghai Jiao Tong University</i>)	
• POSTER: Authenticated Secret Key Extraction Using Channel Characteristics for Body Area Networks	1028
Jiawei Yuan, Lu Shi, Shucheng Yu (<i>University of Arkansas at Little Rock</i>), Ming Li (<i>Utah State University</i>)	
• POSTER: Privacy Preserving Boosting in the Cloud with Secure Half-Space Queries	1031
Shumin Guo, Keke Chen (<i>Wright State University</i>)	
• POSTER: Detecting Money-Stealing Apps in Alternative Android Markets	1034
Chao Yang (<i>Texas A&M University</i>), Vinod Yegneswaran, Phillip Porras (<i>SRI International</i>), Guofei Gu (<i>Texas A&M University</i>)	
• POSTER: Automatic Generation of Vaccines for Malware Immunization	1037
Zhaoyan Xu, Jialong Zhang, Guofei Gu (<i>Texas A&M University</i>), Zhiqiang Lin (<i>University of Texas</i>)	
• POSTER: A Covert Channel Construction in a Virtualized Environment	1040
Jidong Xiao, Zhang Xu (<i>The College of William and Mary</i>), Hai Huang (<i>IBM T.J. Watson Research Center</i>), Haining Wang (<i>The College of William and Mary</i>)	
• POSTER: Robust Dynamic Remote Data Checking for Public Clouds	1043
Bo Chen, Reza Curtmola (<i>New Jersey Institute of Technology</i>)	
• POSTER: Model-Based Context Privacy for Personal Data Streams	1046
Supriyo Chakraborty, Kasturi Rangan Raghavan (<i>University of California, Los Angeles</i>), Mani Srivastava (<i>University of California, Los Angeles</i>), Harris Teague (<i>Qualcomm Inc.</i>)	
• DEMO: Query Encrypted Databases Practically	1049
Dongxi Liu, Shenlu Wang (<i>CSIRO ICT Centre</i>)	

Tutorials

- **Hardware Enhanced Security** 1052
Ruby Lee (*Princeton University*), Simha Sethumadhavan (*Columbia University*),
G. Edward Suh (*Cornell University*)
- **The State and Evolution of Privacy by Design** 1053
Stuart S. Shapiro (*The MITRE Corporation*)
- **Large-Scale DNS Data Analysis** 1054
David Dagon (*Georgia Institute of Technology*)

Workshops

- **Fifth ACM Workshop on Artificial Intelligence and Security (AISec 2012)** 1056
Alvaro A. Cárdenas (*Fujitsu Laboratories of America*), Blaine Nelson (*University of Tübingen*),
Benjamin I. P. Rubinstein (*Microsoft Research, Silicon Valley*)
- **STC 2012: The Seventh ACM Workshop on Scalable Trusted Computing** 1058
Xinwen Zhang (*Huawei Research Center*), Xuhua Ding (*Singapore Management University*)
- **4th Cloud Computing Security Workshop (CCSW 2012)** 1060
Srdjan Čapkun (*ETH Zurich*), Seny Kamara (*Microsoft Research*)
- **CCS'12 Co-Located Workshop Summary for SPSM 2012** 1062
William O Enck, Xuxian Jiang (*North Carolina State University*)
- **11th Workshop on Privacy in the Electronic Society** 1064
Nikita Borisov (*University of Illinois at Urbana-Champaign*)
- **Second Workshop on Building Analysis Datasets
and Gathering Experience Returns for Security (BADGERS'12)** 1066
Mihai Christodorescu (*IBM T.J. Watson Research Center*)

- Book 2 Author Index** 1068

ACM CCS 2012 Conference Organization

- General Chair:** Ting Yu (North Carolina State University, USA)
- Program Co-chairs:** George Danezis (Microsoft Research Cambridge, UK)
Virgil Gligor (Carnegie Mellon University, USA)
- Tutorial Co-chairs:** Brent Byunghoon Kang (George Mason University, USA)
Adam J. Lee (University of Pittsburgh, USA)
- Workshop Co-chairs:** V.N. Venkatakrishnan (University of Illinois at Chicago, USA)
Apu Kapadia (Indiana University, USA)
- Treasurer:** Xuxian Jiang (North Carolina State University, USA)
- Proceedings Chair:** Murat Kantarcioglu (University of Texas at Dallas, USA)
- Web Chair:** Weichao Wang (University of North Carolina at Charlotte, USA)
- Student Travel Grant Co-chairs:** Ragib Hasan (University of Alabama at Birmingham, USA)
Zhenkai Liang (National University of Singapore, Singapore)
- Posters and Demo Co-chairs:** Haining Wang (College of William and Mary, USA)
Nan Zhang (The George Washington University, USA)
- Publicity Co-chairs:** Nicola Zannone (University of Eindhoven, Netherlands)
Wentao Zhu (Chinese Academy of Sciences, China)
- Patrons & Industry Outreach Committee:** Mladen Vouk (North Carolina State University, USA)
Peng Ning (North Carolina State University, USA)
Landon Cox (Duke University, USA)
Xintao Wu (University of North Carolina at Charlotte, USA)
- Local Arrangements Chair:** Michael Rappa (North Carolina State University, USA)
- Local Arrangements Committee:** Laurie Williams (North Carolina State University, USA)
William Enck (North Carolina State University, USA)
Douglas Reeves (North Carolina State University, USA)
Xiaohong Yuan (North Carolina A&T, USA)
Mohamed Shehab (University of North Carolina at Charlotte, USA)
- Steering Committee Chair:** Elisa Bertino (Purdue University, USA)
- Steering Committee:** Carl Landwehr (University of Maryland, USA)
John Mitchell (Stanford University, USA)
Rei Safavi-Naini (University of Calgary, Canada)
Giovanni Vigna (University of California Santa Barbara, USA)
Marianne Winslett (University of Illinois at Urbana-Champaign, Singapore)

Program Committee: Giuseppe Ateniese (Sapienza-University of Rome, Italy
and Johns Hopkins University, USA)
Michael Backes (Saarland University and MPI-SWS, Germany)
Adam Barth (Stanford University, USA)
David Basin (ETH Zurich, Switzerland)
Konstantin Beznosov (U. of British Columbia, Canada)
Bruno Blanchet (CNRS, ENS, INRIA, France)
Alexandra Boldyreva (Georgia Institute of Technology, USA)
Nikita Borisov (University of Illinois at Urbana-Champaign, USA)
Jan Camenisch (IBM Research Zurich, Switzerland)
Srdjan Capkun (ETH Zurich, Switzerland)
Claude Castelluccia (INRIA, France)
Shuo Chen (Microsoft Research, USA)
Mihai Christodorescu (IBM Research, USA)
Richard Clayton (University of Cambridge, England)
Veronique Cortier (LORIA INRIA-Lorraine, France)
Riccardo Focardi (University of Venice, Italy)
Bryan Ford (Yale University, USA)
Phillipe Golle (Google, USA)
Andy Gordon (Microsoft Research, USA)
Guofei Gu (Texas A&M University, USA)
Thorsten Holz (Ruhr-University Bochum, Germany)
Nicholas Hopper (University of Minnesota, USA)
Jean-Pierre Hubaux (EPFL, Switzerland)
Sotiris Ioannidis (Foundation for Research and Technology, Greece)
Sushil Jajodia (George Mason University, USA)
Markus Jakobsson (PayPal, USA)
Jonathan Katz (University of Maryland, USA)
Stefan Katzenbeisser (TU Darmstadt, Germany)
Angelos Keromytis (Columbia University, USA)
Engin Kirda (Northeastern University, USA)
Arvind Krishnamurthy (University of Washington, USA)
Ralf Kuesters (University of Trier, Germany)
Peeter Laud (Cybernetica, Norway)
Wenke Lee (Georgia Institute of Technology, USA)
Ninghui Li (Purdue University, USA)
Benjamin Livshits (Microsoft Research, USA)
Heiko Mantel (TU Darmstadt, Germany)
Patrick McDaniel (Pennsylvania State University, USA)
Tyler Moore (Wellesley College and SMU, USA)
Andrew C. Myers (Cornell University, USA)
Alina Oprea (RSA Laboratories, USA)
Bryan Parno (Microsoft Research, USA)

Program Committee (continued): Kenny Paterson (Royal Holloway, U. of London, England)
Adrian Perrig (Carnegie Mellon University, USA)
Frank Piessens (KU Leuven, Belgium)
Niels Provos (Google, USA)
Christian Rechberger (DTU, Denmark)
Mike Reiter (University of North Carolina at Chapel Hill, USA)
Thomas Ristenpart (University of Wisconsin, USA)
Deng Robert (Singapore Management University, Singapore)
Ahmad-Reza Sadeghi (TU Darmstadt and Fraunhofer SIT Darmstadt, Germany)
Radu Sion (Stony Brook University, USA)
Anil Somayaji (Carleton University, Canada)
Salvatore J. Stolfo (Columbia University, USA)
Paul Syverson (Naval Research Laboratory, USA)
Ingrid Verbauwhede (KU Leuven, Belgium)
Michael Waidner (CASED, Germany)
Dan Wallach (Rice University, USA)
Helen Wang (Microsoft Research, USA)
Bogdan Warinschi (University of Bristol, UK)
Haifeng Yu (National University of Singapore, Singapore)

CCS 2012 Additional Reviewers

Michel Abdalla	Rui Chen	Marc Fischlin	Chang-Han Jong
Gergely Acs	Ashish Choudhary	Connor Fitzsimons	Joshua Juen
Markus Aderhold	Richard Chow	AurÈlien Francillon	Lukas Kalabis
Berker Agir	Bruno Concinha	Matt Fredrikson	Liina Kamm
Mihhail Aizatulin	Mauro Conti	David Galindo	Ian Kash
Massimiliano Albanese	Henry Corrigan-Gibbs	Chris Gates	Vasileios P. Kemerlis
Cory Altheide	Crispin Cowan	Richard Gay	Abdullah Abdul Khadir
Elli Androulaki	Jason Crampton	Essam Ghadafi	Hyoungshick Kim
Claudio Agostino	Cas Cremers	Marco Ghiglieri	Yongdae Kim
Ardagna	Weidong Cui	Benedikt Gierlichs	Felix Klaedtke
Owen Arden	Reza Curtmola	Xun Gong	Markulf Kohlweiss
Frederik Armknecht	Bandan Das	Sylvia Grewe	Clemens Kolbitsch
Elias Athanasopoulos	Anupam Das	Thomas Gross	Vladimir Kolesnikov
Amittai Aviram	Mohammad Torabi	Ramakrishna Gummadi	Georgios Kontaxis
Erman Ayday	Dashti	Aditi Gupta	Aleksandra Korolova
Sumeet Bajaj	Marion Daubignard	Andreas Haeberlen	Steve Kremer
Josep Balasch	Luca Davi	Pierre-Cyrille Heam	Stephan Krenn
Lucas Ballard	Alessandra De Benedictis	Kevin Henry	Markus Kuhn
Gergei Bana	Willem De Groef	Victor Heorhiadi	Taekyoung Kwon
Endre Bangerter	Philippe De Ryck	Cormac Herley	Junzuo Lai
Ian Batten	Lieven Desmet	Jens Hermans	Tobias Lauinger
Lujo Bauer	Dominique Devriese	Stephan Heuser	Sven Laur
Santiago Zanella	Sabrina De Capitani Di	Theodora Hinkle	William Leddy
BÈguelin	Vimercati	Daniel Holcomb	Soo Bum Lee
Alastair Beresford	Alexandra Dmitrienko	Matthias Hollick	Yingjiu Li
Sebastian Biedermann	Maria Dubovitskaya	Amir Houmansadr	Zhiqiang Lin
Igor Bilogrevic	Tran Dung	Yih-Chun Hu	Donggang Liu
Nathaniel Boggs	Alan Dunn	Lin-Shung Huang	Jacob Lorch
Joseph Bonneau	Francois Dupressoir	KÈvin Huguenin	Steffen Lortz
Luis Brandao	Alfredo Rial Duran	Mathias Humbert	Flaminia Luccio
Christina Brzuska	Matthew Edman	John Ioannidis	Daniel Luchaup
Sven Bugiel	Manuel Egele	Yuval Ishai	Alexander Lux
Samuel Burri	Norbert Egi	Pooya Jaferian	Roel Maes
Elie Bursztein	Moussa Ehsan	Geetha Jagannathan	Sergio Maffeis
Kevin Butler	William Enck	Suman Jana	Ken Mai
Christian Cachin	Robert Enderlein	Rob Jansen	Luka Malisa
David CadÈ	Sarah Ereth	Marek Jawurek	Claudio Marforio
David Cash	Sebastian Faust	Kangkook Jee	Srdjan Marinovic
Lorenzo Cavallaro	Martin Feldhofer	Alan Jeffrey	Ramya Masti
Sambuddho Chakravarty	Adrienne Felt	Limin Jia	Ilya Mironov
Haining Chen	Daniel Fett	Aaron Johnson	Chris Mitchell
Jing Chen	Dario Fiore		

Prateek Mittal	Radha Poovendran	Ben Smyth	Margus Veanes
Prashanth Mohan	Christina Popper	Dieter Sommer	Andreas Vogt
Alexander Moshchuk	Donald E. Porter	Yingbo Song	Nevena Vratonjic
Jan Tobias Muehlberg	Georgios Portokalidis	Claudio Soriente	Colin Walter
Madeline Gonzalez	Franz-Stefan Preiss	Alessandro Sornioti	Lingyu Wang
Muniz	Sasa Radomirovic	Christoph Sprenger	Qiyang Wang
Steven Murdoch	Moheeb Abu Rajab	Artem Starostin	Rui Wang
Ildar Muslukhov	Aanjhan Ranganathan	Graham Steel	Xiaofeng Wang
Chanathip Namprempre	Mariana Raykova	Martin Stopczynski	Xinyuan Wang
Gregory Neven	Joel Reardon	Raoul Strackx	Lei Wei
Siaw-Lynn Ng	Rob Reeder	Henning Sudbrock	Jan Willemson
Margus Niitsoo	Tamara Rezk	Kun Sun	David Wolinsky
Nick Nikiforakis	Franziska Roesner	San-Tsai Sun	Hongjun Wu
Peng Ning	Phillip Rogaway	Ewa Syta	Yinglian Xie
Cristina Nita-Rotaru	Carsten Rudolph	Riivo Talviste	Xinyu Xing
Guevara Noubir	P. Y. A. Ryan	Erik Tews	Zhaoyan Xu
Michael Nowlan	Jens Sauer	Abhradeep Thakurta	Qiang Yan
Stefan Nuernberger	Marios Savvides	George	Chao Yang
Damien Oteau	Guillaume Scerri	Theodorakopoulos	Liu Yang
Kaan Onarlioglu	Sebastian Schrittwieser	Nils Tippenhauer	Ting-Fang Yen
Adam O'Neill	Dominique Schroder	Wade Trappe	Scott Yilek
Miriam Paiola	Steffen Schulz	Patrick Traynor	Michal Zalewski
Vasilis Pappas	Matthias Schunter	Nikos Triandopoulos	Davide Zanetti
Michael Pedersen	Gambs Sebastien	Carmela Troncoso	Angelika Zavou
Roel Peeters	Vyas Sekar	Tomasz Truderung	Ennan Zhai
Olivier Pereira	Elaine Shi	Max Tuengerthal	Bingsheng Zhang
Daniele Perito	Ji Sun Shin	Markus Ullrich	Jialong Zhang
Matthias Perner	Seungwon Shin	Steven Van Acker	Xin Zhang
Andreas Peter	Reza Shokri	Marten Van Dijk	Yinqian Zhang
Pieter Philippaerts	Hossein Siadati	Anthony Van Herrewege	Jun Zhao
Krzysztof Pietrzak	Hervais Simo	Jan Van Houdt	Sencun Zhu
Massimiliano Poletto	Dave Singelee	Guy Vandenbosch	
Michalis Polychronakis	Sergei Skorobogatov	Serge Vaudenay	

ACM CCS 2012 Sponsor & Supporters

Sponsor:



Supporters:

