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

Advancing Computing as a Science & Profession

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

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, Illnois, 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

Session 5: Anonymous Communications

Session 6: Web Security

Session 7: Malware and Intrusion Detection

Session 8: Formal Methods and Verification

Keynote Address

Session 9: Virtual Machines and Hypervisors

Session 10: Applied Cryptography

Session 11: Wild Woolly Web

Session 12: Cloud Computing

Session 13: Side-channel Attacks and Defenses

Session 14: Securing Web Applications

Session 15: Privacy and Mobile Security

Session 16: Making Secure Computation Practical

Poster and Demo Session

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

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

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

CCS 2011 Sponsor & Supporters

Sponsor:

Supporters:

NORTHWESTERN
UNIVERSITY