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

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 from 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

Session 4: Software Security

Session 5: Mobile Security

Session 6: Cloud Security

Session 7: Intrusions & Abuse

Session 8: Usability, Authentication & Trust

Session 9: Infrastructure Security & Privacy

Session 10: Applied Cryptography I

Session 14: Verification

Session 15: Web Security

Session 16: Secure Computation

Session 17: Badware

Session 18: Theory

Session 19: Payments, Votes & Reputation

Session 20: Applied Cryptography II

Posters & Demos

Tutorials

Workshops

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

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

ACM CCS 2012 Sponsor & Supporters

Sponsor:

Supporters: