CCSW 2009: The ACM Cloud Computing Security Workshop

in conjunction with the 16th ACM Conference on Computer and Communications Security (CCS)
13 November 2009, Hyatt Regency Chicago, Chicago, IL

registration | speakers | program | organizers | CFP (pdf)

Check out CCSW 2010.

Notwithstanding the latest buzzword (grid, cloud, utility computing, SaaS, etc.), large-scale computing and cloud-like infrastructures are here to stay. How exactly they will look like tomorrow is still for the markets to decide, yet one thing is certain: clouds bring with them new untested deployment and associated adversarial models and vulnerabilities. It is essential that our community becomes involved at this early stage. The CCSW workshop aims to bring together researchers and practitioners in all security aspects of cloud-centric and outsourced computing, including:

- secure cloud resource virtualization mechanisms
- secure data management outsourcing (e.g., database as a service)
- practical privacy and integrity mechanisms for outsourcing
- foundations of cloud-centric threat models
- secure computation outsourcing
- remote attestation mechanisms in clouds
- sandboxing and VM-based enforcements
- trust and policy management in clouds
- secure identity management mechanisms
- new cloud-aware web service security paradigms and mechanisms
- cloud-centric regulatory compliance issues and mechanisms
- business and security risk models and clouds
- cost and usability models and their interaction with security in clouds
- scalability of security in global-size clouds
- trusted computing technology and clouds
- binary analysis of software for remote attestation and cloud protection
- network security (DOS, IDS etc.) mechanisms for cloud contexts
- security for emerging cloud programming models
- energy/cost/efficiency of security in clouds

We would like to especially encourage novel paradigms and controversial ideas that are not on the above list. The workshop is to act as a fertile ground for creative debate and interaction in security-sensitive areas of computing impacted by clouds.

Location News

The workshop takes place in the Toronto room.

Student Stipends

Student stipends are available to attend CCSW. Please apply on the CCS website and mention CCSW as your target workshop. We plan on awarding **2-7 student travel grants (a function also of the quality of the applications).**

Speakers

Whitfield Diffie
Visiting Professor
Royal Holloway College
University of London

Whitfield Diffie is currently a Visiting Professor at the Royal Holloway College, University of London. Best known for his 1975 discovery of the concept of public key cryptography, Whitfield Diffie spent the 1990s working primarily on the public policy aspects of cryptography and has testified several times in the Senate and House of Representatives. His position - in opposition to limitations on the business and personal use of cryptography - is the subject of the book, _Crypto_, by Steven Levy of Newsweek. Diffie and Susan Landau are joint authors of the book Privacy on the Line, which examines the politics of wiretapping and encryption and won the Donald McGannon Award for Social and Ethical Relevance in Communications Policy Research and the IEEE-USA award for Distinguished Literary Contributions Furthering Public Understanding of the Profession. Diffie has also been a Sun Microsystems Vice President and Fellow, as well as its Chief Security Officer. As a CSO, Diffie was the chief exponent of Sun's security vision and responsible for developing Sun's strategy to achieve that vision. Diffie is a fellow of the Marconi Foundation and is the recipient of awards from a number of organizations, including IEEE, The Electronic Frontiers Foundation, NIST, NSA, the Franklin Institute and ACM. Diffie received a Bachelor of Science degree in mathematics from the Massachusetts Institute of Technology in 1965, and was awarded a Doctorate in Technical Sciences (Honoris Causa) by the Swiss Federal Institute of Technology in 1992.

Ian Foster
Associate Division Director, MCS
Director, CI
Argonne National Laboratory

Ian Foster is considered one of the founders of the international Grid community and has written many influential documents on Grid architecture and principles. He created the Distributed Systems Lab at Argonne and University of Chicago, which has pioneered key Grid concepts, developed Globus software, the most widely deployed Grid software, and led the development of successful Grid applications across the sciences. An internationally recognized and widely cited researcher, Foster is a fellow of the American Association for the Advancement of Science and the British Computer Society. With Dr. Carl Kesselman, he co-edited The Grid 2: Blueprint for a New Computing Infrastructure, now in its second edition (Morgan Kaufmann, 2003). Foster graduated with a B.S. in computer science from the University of Canterbury, New Zealand and a Ph.D. in computer science from Imperial College, United Kingdom.

Peter Mell
Project Lead, Cloud Computing Security

National Institute of
Standards and Technology
NIST
...working with industry to foster innovation, trade, security and jobs

National Institute of Standards and Technology (NIST)
Computer Security Division

Peter Mell is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST). He is the cloud computing and security project lead at NIST and is the lead author on NIST's upcoming cloud guidance publication. He is also the creator of the National Vulnerability Database and the Security Content Automation Protocol (SCAP) validation program. These programs are widely adopted within the U.S. government and industry and used for standardizing and automating vulnerability and configuration management, measurement, and policy compliance checking. His research experience includes the areas of cloud computing, security metrics, security automation, vulnerability databases, and intrusion detection systems (IDSs).

Program (preliminary)

07:30 - 08:00 **Breakfast**

08:00 - 08:20 **Chair's Welcome and Opening Remarks** (pdf)

08:20 - 09:40 **Research Session: Web 2.0** (Chair: *Dawn Song, UC Berkeley*)

Peifung Lam, Elie Bursztein, John Mitchell, "TrackBack Spam: Abuse and Prevention" (slides)

Francis Hsu, Hao Chen, "Secure File System Services for Web 2.0 Applications"

Jennifer Sobey, Tara Whalen, Robert Biddle, Paul Van Oorschot, Andrew Patrick, "Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study" (slides)

Dominik Herrmann, Rolf Wendolsky, Hannes Federrath, "Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naive-Bayes Classifier" (slides)

09:40 - 09:45 **Short Break**

09:45 - 10:35 **Invited Talk:** Whitfield Diffie, Royal Holloway College, University of London

Plus ca Change: Security in the Ether; Security in the Cloud
The security implications of cloud computing can best be understood by looking back a century to the introduction of radio. On one hand, radio provided a medium of communication without which no competitor (in business or in war) could expect to prevail. On the other, it bypassed all of the information-security measures in active use at the time. The security of radio was rescued by a long known but irregularly applied technology: cryptography. Cloud computing will permit computing to be easily outsourced, lowering costs and increasing flexibility. As with radio this will be so valuable that no one can expect to survive in business without it but the security challenge it presents is different. Cloud computing does not directly deny you control over the people with whom you share your information but it forces you to share it with people not entirely of your choosing. A pure technological fix seem unlikely to solve this problem and cloud computing will require an unprecedented integration of the legal and procedural frameworks for computing transactions.

10:35 - 11:00 **Coffee Break**

11:00 - 12:00 **Research Session: Data Outsourcing** (Chair: *Peter Williams, Stony Brook University*)

Alina Oprea, Kevin Bowers, Ari Juels, "Proofs of Retrievability: Theory and Implementation" (slides)

Weichao Wang, Zhiwei LI, Rodney Owens, Bharat Bhargava, Mark Linderman, "Secure and Efficient Access to Outsourced Data" (slides)

Aaram Yun, Chunhui Shi, Yongdae Kim, "On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage" (slides)

12:00 - 12:05 **Short Break**

12:05 - 12:55 **Invited Talk:** Ian Foster, Argonne National Laboratory

12:55 - 13:40 **Lunch and Mingle**

13:40 - 13:50 **Message from Sponsor:** Kristin Lauter, Microsoft Research

Cryptographic Cloud Storage (slides)
We present a proposal for cryptographic cloud storage design based on emerging cryptographic technologies. We discuss the benefits and motivations for such a design, including applications like privacy for electronic medical records and systems for scientific publishing of large data sets. This is work with Seny Kamara.

13:50 - 14:00 **Invited Speaker:** Lenore Zuck, National Science Foundation

14:00 - 15:25 **Research Session: New Challenges** (Chair: *Bogdan Carbunar, Motorola Labs*)

Himanshu Raj, Ripal Nathuji, Abhishek Singh, Paul England, "Resource Management for Isolation Enhanced Cloud Services" (slides)

Short Paper: Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Elaine Shi, Jessica Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control" (slides)

Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapa, Sangoh Jeong, "Securing Elastic Applications on Mobile Devices for Cloud Computing" (slides)

Short Paper: Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning, "Managing Security of Virtual Machine Images in a Cloud Environment" (slides)

Short Paper: Mihai Christodorescu, Reiner Sailer, Douglas Schales, Daniele Sgandurra, Diego Zamboni, "Cloud Security Is Not (Just) Virtualization Security" (slides)

15:25 - 15:55 **Coffee Break**

15:55 - 16:45 **Invited Talk:** Peter Mell and Tim Grance, NIST

Effectively and Securely Using the Cloud Computing Paradigm (slides)
This presentation will discuss the National Institute of Standards and Technologies' definition of cloud computing which has been widely adopted within the U.S. government. It will then use that definition as a framework on which to reason about cloud security advantages and challenges.

16:45 - 16:50 **Short Break**

16:50 - 17:30 **Research Session: Applications** (Chair: *Cristina Nita-Rotaru, Purdue University*)

Melissa Chase, Kristin Lauter, Josh Benaloh, Eric Horvitz, "Patient Controlled Encryption: patient privacy in electronic medical records"

Mariana Raykova, Binh Vo, Steven Bellovin, Tal Malkin, "Secure Anonymous Database Search" (slides)

17:30 **Conclusion**

Registration

Please register here on the main CCS website.

Organizers

STEERING
Radu Sion, Stony Brook (chair)
Gene Tsudik, UC Irvine
Moti Yung, Google Inc.

CHAIRS
Radu Sion, Stony Brook (PC chair)
Dawn Song, UC Berkeley (PC co-chair)

COMMITTEE
Bogdan Carbunar, Motorola Labs
George Danezis, Microsoft Research
Roger Dingledine, The Tor Project
Tal Garfinkel, VMware Inc.
Philippe Golle, Palo Alto Research Center
Seny Kamara, Microsoft Research
Angelos Keromytis, Columbia University
Susan Landau, Sun Microsystems Inc.
Wenke Lee, Georgia Tech
Cristina Nita-Rotaru, Purdue University
Patrick McDaniel, Penn State University
Dimitris Papadias, Hong Kong University of Science and Technology
Adrian Perrig, Carnegie Mellon University
Pierangela Samarati, University of Milano
Reiner Sailer, IBM Research
Gene Tsudik, UC Irvine
Nicholas Weaver, ICSI
Peter Williams, Stony Brook
Giovanni Vigna, UCSB
Moti Yung, Google Inc.

Sponsorship

Interested in sponsoring CCSW (this or next year)? Please contact us directly.

Gold Sponsors

NSF

Microsoft Research

Updated: November 28, 2009