



**Association for
Computing Machinery**

Advancing Computing as a Science & Profession

Contact:

Virginia Gold
ACM
212-626-0505
vgold@acm.org

CACM REPORTS: BALANCING SECURITY AND ACCESSIBILITY IN WEB BROWSERS

May Issue also Examines Changing Role of Software Developers

NEW YORK, NY, May 7, 2009 – Designers of modern browsers must defend against evolving threats and well-organized forces seeking to exploit browser vulnerabilities. Browsers, which are at the heart of the Internet experience, are instrumental in maintaining reliable security measures so that users can conduct banking and shopping transactions, display a wide variety of media, and update in real time without compromising sensitive information. In its cover story, the May 2009 issue of *Communications of the ACM* (CACM <http://cacm.acm.org/magazines/2009/5>) weighs security vs. usability and highlights some promising solutions for browser designers. The issue also features excerpts from blog posts <http://cacm.acm.org/blogs> on *Communications'* new Web platform that are updated daily to complement the print content. *Communications*, the flagship publication of ACM, offers readers access to this generation's most significant leaders and innovators in computing and information technology, and is available online in digital format <http://mags.acm.org/communications/200905>.

In an article entitled "Spending Moore's Dividend" about the impact of multicore computers on software developers, author James Larus of Microsoft Research surveys the 30-year era of steady growth in software performance attributable to computing increases predicted by Moore's Law. He points to a historic transition from sequential to parallel computation with the introduction of multicore processors in 2004, and concludes that the burden of software performance has shifted from chip designers and processor architects to software developers.

"Lest We Remember: Cold-Boot Attacks on Encryption Keys" examines threats to laptop users who rely on disk encryption. It describes the underlying vulnerabilities of dynamic random access memory (DRAM), which retains its contents for several seconds after power is lost. Author Alex Halderman of the University of Michigan and his team contend that this phenomenon limits the ability of an operating system to protect cryptographic key material from attackers with physical access to the machine. The team demonstrates how to break BitLocker, the disk encryption utility in Microsoft Vista, which was believed to be strong because the master keys are kept in the trusted platform module known as the TPM chip on the motherboard while the machine is powered down.

An accompanying perspective, "A Chilly Sense of Security," by author Ross Anderson of the University of Cambridge, England finds that this research will change the way people write and test security software, and concludes that software engineers who build security applications must understand the hardware as well as the software and the people who use it.

An article on 'Algorithmic Systems Biology' surveys the convergence of computer science and biology, and finds that while computing has become a resource for biology that has led to the field of bioinformatics, the reverse direction is also proceeding. Biology is experiencing a heightening of interest in system dynamics by interpreting living organisms as information manipulators. According to author Corrado Priami of the Microsoft Research-University of Trento Centre for Computational and Systems Biology, this "systems biology" approach embraces a transition to mathematical modeling that incorporates algorithms and the programming languages used to specify them. The convergence between computing and systems biology, he continues, offers a valuable opportunity that can fuel the discovery of solutions to many of the current challenges in both fields.

In "Matchmaker, Matchmaker," an essay on the rapidly changing advertisements that appear on Web pages explains a new discipline called computational advertising. Science writer David Essex describes this development as a type of automation that tries to replicate what humans might do if they had the time to read Web pages to discern content and find relevance. Currently, electronic auctions employed by Google, MSN, and Yahoo! assign ads to their own results pages and the pages of other Web sites with the goal of achieving the best match for sponsored search ads, banner ads, and contextual advertising in the best context before the right customer. The author reviews promising avenues these companies are pursuing to understand the intent of people exposed to ads.

Other May *Communications* articles:

- "The Network Neutrality Debate Hits Europe" discusses the differences in telecommunications regulation between the U.S. and the European Union and their impact on the network neutrality debate.
- "Teaching Computing to Everyone" examines the lessons learned from creating high-demand computer science courses for non-computing majors.
- "Debugging AJAX in Production" proposes design principles for debugging the JavaScript language known as AJAX to manage the proliferation of sophisticated AJAX web development techniques that are used to create interactive web applications or rich Internet applications.
- At BLOG@CACM, bloggers Greg Linden, Jason Hong, Michael Stonebraker and Mark Guzdial discuss recommendation algorithms, online privacy, scientific databases, and programming in introductory computer science classes. Excerpts from their recent posts plus readers' comments are published in this issue.
- In two blogs, Editor-in-Chief Moshe Vardi weighs the current reliance on conference publications as the primary means of publishing computer research, and provokes a lively online debate over whether this system is serving the community well. (<http://weblog.fortnow.com/2009/04/vardi-are-conferences-worth-fixing.html> and <http://agtb.wordpress.com/2009/04/25/on-vardis-question-on-conferences/>)

About ACM

ACM, the Association for Computing Machinery www.acm.org, is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and

recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###