



## From the Newsstand

Alison Skratt

### Elsewhere in the IEEE Computer Society

#### Computer

[www.computer.org/computer/](http://www.computer.org/computer/)  
February 2006

**“New Flash Player Rises in the Web-Video Market,”**  
by **Jacqueline Emigh**

The “big three” — Real Networks’ RealPlayer, Microsoft’s Windows Media Player, and Apple’s QuickTime — have long dominated the market for Web video, but Adobe’s Flash is now making a strong challenge. Even before Adobe bought Macromedia in December for US\$3.4 billion, Flash was starting to venture beyond the realm of Web site animation.

Flash 8 includes the Flash Player 8 and Flash Professional 8, a tool for creating content. Unlike the big three, Flash players also work well with animation and vector graphics. Adobe is pushing Flash for on-demand video streaming because it seems to work best with video embedded into pages and streamed to Web browsers via media servers. As a result, analysts believe it could become increasingly popular in that niche, but probably won’t grow into other areas unless Adobe adds major features, such as streaming live content and support for more file formats.

**“False Domain-Name Database Information Plagues Internet,”**  
by **Linda Dailey Paulson**

A recent investigation by the US Gov-  
*continued on p. 9*

### E-Commerce

#### PC Magazine

[www.pcmag.com](http://www.pcmag.com)  
7 March 2006

**“Net to the Rescue,”**  
by **Sebastian Rupley**

Until recently, the scope of the Internet’s role in personal decisions has been unclear. Yet, in a recent survey of 2,200 adults by the Pew Internet &

American Life Project, 45 percent said the Internet “played a crucial role” in how they made a major life decision in the past two years — up from 33 percent three years ago. Among the types of information those surveyed sought out were advice on finances, cars, career training, and medical information.

### Internet Media

#### PC Magazine

[www.pcmag.com](http://www.pcmag.com)  
11 April 2006

**“Net Film Distribution Coup,”**  
by **Sebastian Rupley**

New technology from start-up Itiva looks like it could play a pivotal role in efforts to bring Hollywood to the Web. Itiva’s Quantum Streaming technology breaks up high-definition (HD) video into http-based Web

pages that can be cached at an ISP in the same way as regular Web pages. In a demonstration, Itiva’s president downloaded a two-minute HD movie trailer at 5.5 Mbits per second (Mbps) in just seconds. If that speed is typical, users could potentially download a 90-minute movie in less than 15 minutes. One major studio has already signed Itiva to distribute its content.

### Mobile and Wireless Computing

#### PC Magazine

[www.pcmag.com](http://www.pcmag.com)  
7 March 2006

**“HyperMegaSuper Wireless?”**  
by **Sebastian Rupley**

Like Wi-Fi, ultrawideband (UWB) uses radio technology, but with claims of more than 480-Mbps delivery speeds, it could facilitate short-range options

such as wireless transfer of images between digital cameras and PCs. For now, however, the WiMedia Alliance and the UWB Forum are pursuing competing standards. Despite the lack of official certification standards, several firms touted their UWB offerings at the recent Consumer Electronics Show and at MacWorld — an increas-

ingly common practice among wireless-product vendors.

**Technology Review**  
[www.technologyreview.com](http://www.technologyreview.com)  
**March/April 2006**  
**“Underground Wi-Fi,”**

by **Patric Hadenius**

Wi-Fi has made the Internet available 1,000 feet underground. Coal, iron, and copper mines across the world are using broadband to retrieve information that helps improve productivity and worker safety. By early 2007, for example, an iron-ore mine located 150 kilometers north of the Arctic Circle in Sweden will have a network of Wi-Fi-linked drills. And copper and coal mines in Germany and Chile are in the process of installing hundreds of Wi-Fi hotspots.

In addition to creating a reliable link to the world above, the networks also mean fewer individuals need to be underground because drill and truck location data and truck-load weights can be wirelessly transferred above ground.

**“Cognitive Radio,”** by **Neil Savage**

Every year, *Technology Review* details 10 emerging technologies worth watching. One of this year’s is cognitive radio. Heather Zheng, an assis-

tant professor of computer science at the University of California, Santa Barbara, believes cognitive radios could help address the growing problem of shrinking Wi-Fi bandwidth because the devices can scan for frequencies that aren’t being used at a given moment and select one or more for transmitting or receiving data. She is working on a way to get cognitive radios to work together, giving priority to the FCC-designated frequency owner, but sharing the rest of the unused spectrum with other cognitive radios.

**“Pervasive Computing,”**

by **Neil Savage**

Savage outlines efforts at a radio test-bed lab at Rutgers University to develop a protocol that standardizes the way remote devices communicate — a key to pervasive computing’s success.

The lab, directed by Dipankar Raychaudhuri, features 800 computers with three radios apiece. Two radios handle Wi-Fi standards, and the third uses either the ZigBee or Bluetooth short-range protocols. When programmers come up with potential protocols, they configure the radios to test how long it takes each to contact the others and send data. The lab’s size lets researchers test for real-world challenges and complexities.

## Security

**IT Architect**  
[www.itarchitect.com](http://www.itarchitect.com)  
**March 2006**

**“Email Payola for AOL, Yahoo,”**

by **Andrew Conry-Murray**

America Online (AOL) has begun a certified email system in which businesses can pay for direct access to users’ inboxes — as long as those receiving the emails agree. AOL is using Goodmail Systems’ technology, which verifies a sender’s identity and adds a “trust symbol” to certified messages. The messages bypass spam filters and

retain images and Web links that are often stripped out of incoming emails. Conry-Murray suggests that Yahoo is testing the Goodmail system as well. AOL says the system will help cut down on phishing and spam by charging companies for legitimate, user-approved access to inboxes. It says the quarter cent to one cent it charges per email will go toward offsetting AOL’s spam-filtering expenses.

**“Maps, the Killer Apps,”**

by **Andy Dornan**

## Elsewhere in the IEEE Computer Society

*continued from p. 8*

ernment Accountability Office estimated that about 5 percent of the 44.9 million registrations for .com, .net, and .org entries contained blatantly false contact information, including fields filled with gibberish. The report said another 2.7 percent of those registrations had incomplete contact information. Domain-name registrars, accredited by the Internet Corporation for Assigned Names and Numbers (ICANN), are responsible only for getting the entries, making them public, and responding to complaints about inaccuracies — all of which they appear to be handling well. For example, statistics show that registrars corrected, suspended, or deactivated more than 60 percent of the accounts for which they received complaints.

**“New Worm Chats Up Its Victims,”** by **Linda Dailey Paulson**

A worm that may be the first to engage its would-be victims in “chats” has been making the rounds. Named IM.Myspace 04.AIM by IMlogic, an enterprise-IM-software firm, the worm affects those who use America Online’s Instant Messenger. It arrives in a missive that appears to come from a member of the recipient’s buddy list who uses the MySpace social-networking site. The message has a link, supposedly to a photo, that sends the user to a Web page hosting the malware. If the recipient responds to the first message, the worm will reply with Internet slang, like “lol thats cool,” orchestrated to perpetuate the illusion that it’s an actual IM exchange.

If the malware reaches the user’s computer, it will send itself, in the background, to everyone on their buddy list. It can also generate executables that relaunch the worm each time the infected computer is turned on, or block online connections used by antivirus software to update virus signatures.

**March 2006**  
**“Sploggers Make Money**

*continued on p. 10*

## Elsewhere in the IEEE Computer Society

continued from p. 9

### by Inflating Search Rankings,” by Linda Dailey Paulson

Now that blogging has joined the mainstream, several fake blogs, called splogs, have popped up. Sploggers manipulate the keywords in their splogs to improve their rankings in search-engine results, which, in turn, increase the likelihood that users will click on the ads on their splogs.

According to Technorati, a blog-tracking search engine, splogs could be inflating the number of blogs by as much as 18 percent. The splogs can feature actual articles, but may also have copied content or simply be gibberish. In those cases, sploggers might hire others to click through on their ads to generate revenue. Other sploggers are making bots that can automatically create splogs, increasing the problem exponentially.

### IEEE Distributed Systems Online <http://dsonline.computer.org> February 2006

#### “Peer-to-Peer: Is Deviant Behavior the Norm on P2P File-Sharing Networks?” by Daniel Hughes, James Walkerdine, Geoff Coulson, and Stephen Gibson

Peer-to-peer (P2P) file-sharing networks, which are moving toward more anonymous, decentralized architectures, provide a unique environment for observing human social behavior because they lack any central authority. Hughes and his coauthors intercepted and analyzed query and query-hit messages to examine the prevalence of illegal pornography on the Gnutella P2P network. Although some researchers suggest that anonymity “generally increases the likelihood” of deviant behavior online, these experiments suggest that only a small but active part of the P2P community is responsible for most of the illegal pornography. Specifically, it found that 1.6 percent of searches and 2.4 percent of responses on the days studied were for

continued on p. 11

A recent study by the Pew Internet & American Life Project shows that looking up directions and maps has become the number one activity on the Internet. So it’s no surprise that Google, Microsoft, Yahoo, and mobile operators have announced plans to unveil new mapping technologies in the near future.

Yet, safety could become an issue when queries are transferred through carriers or other services where they could be stored indefinitely and serve as treasure troves for criminals. To help address this issue, Microsoft has unveiled Location Finder, a free Windows application that triangulates right on a client’s laptop. Location Finder listens without connecting, so it works offline or with commercial hotspots, even if a user doesn’t have an account, thanks to a Wi-Fi hotspot database linked to geographic coordinates.

To run Location Finder, however, users must set their default browsers to Internet Explorer, which opens up other security concerns such as spyware and Trojans. Also, to get an actual map, Location Finder must connect to the Internet and the user must allow the data to be sent to Microsoft.

### PC Magazine [www.pcmag.com](http://www.pcmag.com) 21 March 2006

#### “Who, Me?” by Sebastian Rupley

In the wake of the controversy in which MSN, Yahoo, and Google agreed to adhere to China’s censorship policies, one company is working to free Chinese citizens from its government’s directives. Anonymizer says it will soon release free tools that will let Web users anonymously post information and access the Internet without any filters. The company already helps similar efforts in Iran. Anonymizer’s president says, “Information bounces off a proxy we operate. It encrypts all the traffic and scrambles the URLs, so there’s no trace left on the user’s PC.”

### 11 April 2006 “The Wireless Snare,”

by Robert Lemos

How many times have you worked on your laptop while waiting for a flight? Recent real-world experiments by researcher Mark Loveless show you could be opening yourself up to serious security threats if you do — thanks to your laptop’s default wireless settings.

Loveless came to this conclusion after he began exploring why so many laptops at airports were broadcasting common network names or service set identifiers (SSIDs). He found a “significant portion” of laptops’ default settings were configured to look for and connect to common SSIDs, such as “linksys” or “dlink.” If they find no network, laptops often create their own wireless network using a common SSID and connecting to each other, creating serious security gaps that could let attackers join and control these ad hoc networks and gain access to usernames, passwords, and other confidential information. Lemos examines a three-fold solution: turn off the laptop’s wireless when you’re not trying to connect to a known network; make sure the laptop doesn’t automatically turn on its wireless when it can’t find an Ethernet connection; and disable ad hoc networking.

### Technology Review [www.technologyreview.com](http://www.technologyreview.com) March/April 2006

#### “Jonathan Zittrain: Preempting an Internet Clampdown,”

by David Talbot

Jonathan Zittrain, professor of Internet governance at the University of Oxford and cofounder of Harvard Law School’s Berkman Center for Internet and Society, says it’s easy to envision the day when a single destructive virus does so much damage that governments are forced to enact strict regulations that not only send consumers running to safer,

closed networks but also eliminate amateurs' invaluable contributions to the Internet. To help combat the likelihood that this will take place, Zittrain and fellow academicians have launched StopBadWare.org, a project funded by Google, Sun Microsystems, and Lenovo.

In this Q&A, Zittrain explains what brought us to this point, including an example of a worst-case scenario that could lead to a clampdown on the Internet's unfettered nature. He also describes StopBadWare's goals, which include fostering a better understanding of malware and proposing solutions that don't generate other centralized control issues.

#### "Universal Authentication,"

by David Talbot

Although many technologies compete in the area of Internet authenti-

cation, Shibboleth, an open-standard system used by the research community and universities could soon provide the solution to single-sign-on access to multiple Web sites. It not only lets Web users hop from site to site after signing in only once but also guards users' privacy by passing on only the identifying information that additional sites need.

Shibboleth has been expanding its reach exponentially, growing from use at a few US colleges in 2003 to more than 500 sites around the world in 2005. The system is now moving into commercial circles. Reed Elsevier, for example, has started to offer its university-based subscribers access to its online library through Shibboleth. □

Alison Skratt is a freelance writer based in Oakville, Conn.

## Elsewhere in the IEEE Computer Society

*continued from p. 10*

illegal pornography, suggesting it is far from the behavioral norm on Gnutella.

**IEEE Software**  
[www.computer.org/software/](http://www.computer.org/software/)  
**March/April 2006**

### "Using Wikis in Software Development," by Panagiotis Louridas

Eleven years ago, Ward Cunningham posted the world's first wiki on the Web. He called it "the simplest online database that could possibly work." Since then, wikis have turned out to be one of the most popular tool shells ever based on open-source software. In this article, Louridas gives an overview of the wiki arena, including the basics, how wikis can be used in software development, and a brief description of some popular wiki engines.

## Classified Advertising

**SUBMISSION DETAILS:** Rates are \$110.00 per column inch (\$125 minimum). Eight lines per column inch and average five typeset words per line. Send copy at least one month prior to publication date to: Marian Anderson, Classified Advertising, *IEEE Internet Computing Magazine*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; (714) 821-8380; Email: manderson@computer.org.

**CISCO SYSTEMS, INC.** is accepting resumes for the following positions: **CALIFORNIA: Petaluma.** Hardware Engineer (Ref# PET11C), Software Engineer (Ref # PET21C), **San Jose/Milpitas.** CA Project Managers (to drive and implement web-based software applications to automate and change company's transactions) (Ref# SJ011C), Customer Support Engineers (Ref# SJ21C), EMC Compliance Engineer (to design, test and troubleshoot complex high-speed products, to meet national and international EMC and Telecom requirements) (Ref# SJ31C), Hardware Engineers (Ref# SJ41C), IT Engineer (Ref# SJ51C), IT Project Manager (Ref# SJ61C), Manufacturing Quality Engineer (Ref# SJ71C) Manufacturing Systems Administrator (Ref# SJ81C), Software

Development Manager (Ref# SJ91C) Network Consulting Engineers (Ref# SJ101C) New Product Introduction Engineers (to introduce products with high content of electronics circuitry into production and provide best practices for manufacturability, reliability, testing and costing) (Ref# SJ111C), Software Engineers (Ref# SJ121C), Software/QA Engineers (Ref# SJ131C), Systems Engineers (Ref# SJ141C) Technical Leads (Ref# SJ151C), Technical Marketing Engineers (to market, support, promote company technology to customers and other architectures) (Ref# SJ161C), Test Engineers (Ref# SJ171C), Business Development Manager (Ref # SJ181C), Business Operations Manager (Ref# SJ191C), IMC Demand General Manager (Ref# SJ201C), Marketing Programs Manager (Ref# SJ211C), Field Marketing Specialist (to provide integrated forecast of market opportunities by various dimensions such as technology, geography, customer market segments) (Ref# SJ221C), Program Manager (Ref# SJ251C), Consulting Systems Engineer (Ref # SJ261C), Product Manager (Ref# SJ271C), Financial Analyst (Ref# SJ281C), Engineering Manager (Ref# SJ351C). **San Diego.** Software Engineer (Ref# SD011C). **COLORADO: Boulder.** Customer Support Engineers (Ref# BO11C), Software Engineers (Ref# BO21C). **FLORIDA: Miami.** Sr. Director Operations (Ref# MIA11C),

Marketing Operations Manager (Ref# MIA21C). **GEORGIA: Atlanta.** Area VP, Sales (Ref# ATL011C). **MASSACHUSETTS: Boxborough.** Software Engineers (Ref# BOX11C). **NEW YORK: New York.** Systems Engineer (Ref# NY21C). **NORTH CAROLINA: Research Triangle Park.** Customer Support Engineers (Ref# RTP11C), Network Consulting Engineers (Ref# RTP21C), Quality Systems Engineer (Ref# RTP31C), Software Engineers (Ref# RTP41C), Software/QA Engineers (Ref# RTP51C), Tech Project Systems Engineer (to plan, develop and implement custom test plans for enterprise/service providers and customers) (Ref# RTP61C), Tech Project Systems Specialist (to develop and administer sales training program) (Ref# RTP71C), Technical Lead (Ref# RTP81C), IT Project Manager (Ref# RTP91C), Technical Marketing Engineer (Ref# RTP101C). **TEXAS: Richardson.** Customer Support Engineers (Ref# RIC11C), Network Consulting Engineer (Ref# RIC21C), Software Engineers (Ref# RIC31C), Test Engineer (Ref# RIC41C), Project Manager (Ref# RIC51C). **San Antonio.** Systems Engineer (Ref# SAN11C). Please mail resumes with reference number to Cisco Systems, Inc., Attn: M. Clarke, 170 W. Tasman Drive, Mail Stop: SJC 5/1/4, San Jose, CA 95134. No phone calls please. Must be legally authorized to work in the U.S. without sponsorship. EOE. www.cisco.com.