



From the Newsstand

Alison Skratt

Elsewhere in the IEEE Computer Society

Computer
www.computer.org/computer/
July 2005

“Instant Messaging: A New Target for Hackers,” by Neal Leavitt

As instant messaging systems' popularity has grown, so has the threat from viruses and worms. According to one survey, attacks against major IM networks rose from five in the first quarter of 2004 to 24 in the first quarter of 2005. As with email, IM attacks involve not only viruses and worms, but also phishing, hijacking, and denial-of-service. IM's real-time features make such attacks more dangerous; one simulation last year showed that IM viruses could spread to 500,000 machines in less than 30 seconds. Although major IM networks are working to ensure better memory management to combat this issue, many corporations don't have IM policies, which Leavitt says compounds the problem.

“Securing Wi-Fi Networks,”
by Kjell J. Hole, Erlend Dyrnes,
and Per Thorsheim

The prevalence of Wi-Fi networks based on the IEEE 802.11b/g standard has created an opportunity for hackers to access not only home users' networks but also corporate networks that allow employees home access. The authors conducted a study to assess Wi-Fi networks' security levels in

continued on p. 11

Java

Dr. Dobb's Journal
www.ddj.com
July 2005

“Java & Bluetooth,” by Paul Tremblett

Typically, Bluetooth applications run using Java 2 Micro Edition, but the Bluetooth specification should be able to run on any Java 2 platform, provided that platform offers the Generic Connection Framework. Tremblett, a technical lead at Vonage, outlines how to use the Java Specification Request 82 (www.jcp.org) – which sets a standard API for developing Bluetooth applications with Java – to find nearby Bluetooth devices and determine what services they offer, as well as connect to those devices using well-defined protocols. The result, he says, helps programmers avoid dealing with low-level details while guaranteeing portability.

Dr. Dobb's Journal
www.ddj.com
September 2005

Internet Media

Network Magazine
www.networkmagazine.com
June 2005

“The Incredible VoIP Solution,”
by David Greenfield

To better help network architects evaluate IP private branch exchanges (PBXs), a panel of leading VoIP

“Mobile Java & 3D Apps,”
by Oscar Vivald and Tom Thompson

Mobile phones not only embody the convergence concept, they also act as laboratories for next-generation 3D applications. Vivald and Thompson describe two APIs – HI Corp.'s Masco Capsule Micro3D, version 3 and Java Specification Request (JSR) 184 (which describes the Java 2 Mobile Edition's mobile 3D graphics API) – that Sony Ericsson has included on its phones to encourage widespread 3D application development. Each API has its own approach to creating 3D models quickly without consuming too many platform resources. Vivald and Thompson also explain how to use a few of the APIs' capabilities and recommend that those with modest 3D graphics requirements opt for the Mascot Capsule V3, which they say performs better than the JSR 184 on phones currently available to consumers.

designers and architects created a wish list of telephony requirements. Together, they mapped out what the “incredible VoIP solution” would look like. The panel – including Walt Magnusson, Texas A&M University's director of telecommunications; Michele Narcavage, University of Pennsylva-

nia's voice services project leader; Brian Rosen, president of Emergicom; and Henning Schulzrinne, chair of the Department of Computer Science at Columbia University (and former *IC* editorial board member) — came up with a solution that mixes new functionality with that found in existing VoIP systems. The group defined the system's fully distributed, open architecture and outlined the Session Initiation Protocol network core, while taking into account remote users' needs and integrating remotely managed VoIP and adequate security features. The panel also outlined management solutions that let network architects define global policies, in addition to configurations for individual call servers.

PC Magazine
www.pcmag.com
9 Aug. 2005

“MTV in Overdrive,”

by David Murphy

The cable music channel MTV is offering a new online service (MTV Overdrive) that reaffirms the company's reputation for cultural and technological innovation and offers insight into new ways of combining video broadcasting and the Internet. MTV Overdrive offers largely free video content that users can view like traditional TV, with programs appearing in a predetermined order, or video-on-demand, in which users pick their preferred play lists. Using XML feeds, users can customize Macromedia Flash to power the video streaming. The content is encoded

and compressed using Microsoft's Windows Media codec, which lets MTV lock it up with digital rights management; the majority of the content sits on Sybase databases, and users are ensured fast access to video content through a distributed network of Akamai edge servers.

Technology Review
www.technologyreview
August 2005

“The Business of Blogging,”

by Andrew P. Madden

As weblogs, or blogs, continue to grow in popularity, some entrepreneurs are trying to create business models to profit from them. The Pew Internet and American Life Project conducted a survey in March 2005 and found that 25 percent of respondents had read blogs. Still, finding a successful way to generate profits from this readership isn't easy — to sell advertising, a firm must be able to sell space on the most popular blogs, and, by definition, bloggers are an independent lot who want to be paid up front for their content rather than swap it for equity. The article mentions several established and soon-to-be-launched companies that are trying to profit from blogs nonetheless, including Gawker Media, FM Publishing, BlackInc Media, and Weblogs. It also takes an in-depth look at Weblogs' business model: the company has 80 bloggers in its stable and hopes to ultimately have more than 300 that target technology, media, entertainment, and consumer goods.

Mobile and Wireless Computing

Network Magazine
www.networkmagazine.com
June 2005

“Don't Get Locked In,”

by Andy Dornan

Over the past two years, the Wi-Fi industry has seen both start-ups and established companies produce Wi-Fi

switches used with so-called “thin” access points (APs). Today, most thin APs will work only with vendor-made controllers, inhibiting interoperability. Dornan suggests that, over the next two years, the proprietary architecture of these switches and APs will become less important, giving

Elsewhere in the IEEE Computer Society

continued from p. 10

Bergen, Norway. Using typical hacker techniques — including “walk-by” hacking with a Wi-Fi-enabled PDA — they collected research data without breaking any encryption or revealing the location of any discovered Wi-Fi networks. They found that only 244 of the 706 total identified networks used Wired Equivalent Privacy (WEP), the encryption mechanism developed for Wi-Fi networks. The rest of the networks used little or no encryption. That said, the authors found that even those using WEP code were vulnerable because the WEP code has been broken, and its key is widely available for download. Consequently, the authors strongly urge all corporate and small-office or home-office users to avoid WEP and upgrade to the interim Wi-Fi Protected Access standard created by the Wi-Fi Alliance (www.wi-fi.org). They also suggest that companies avoid connecting access points that use only WEP directly to internal networks, but rather connect all Wi-Fi access points to a separate wired network segment outside the firewall and consider that segment to be insecure.

IEEE Distributed Systems Online
<http://dsonline.computer.org>
May 2005

“Colleges Taking File-Sharing into Their Own Hands,” by Greg Goth

For some time now, college campuses have been hotbeds of illegal file-sharing that not only broke intellectual property laws but also hurt bandwidth availability. Still, universities have a significant need for legitimate file-sharing internally, which has led at least two to work on pioneering technology to help meet that demand. Vassar College is building the Vspace architecture to let small groups of faculty and students share files through a Web browser. Although a client-server environment, rather than a

continued on p. 12

Elsewhere in the IEEE Computer Society

continued from p. 11

P2P network, Vspace will let users post files that others with posting authority can access. Pennsylvania State University has generated worldwide interest in its open-source P2P network, LionShare, which combines file-sharing technology with a mechanism that connects users' activities to their network identification.

June 2005

"Free Riding on Gnutella Revisited: The Bell Tolls?" by Daniel Hughes, Geoff Coulson, and James Walkerdine

Gnutella, a distributed-software project that's created a pure P2P network without a central server, is slowly becoming a victim of its own success. The authors conclude that Gnutella could soon collapse if its developers refuse to crack down on *free riding* — downloading files without contributing any to the network. They outline a new analysis of Gnutella traffic, which updates a 2000 study and shows that free riding has increased significantly since that time, rising to a crisis level. The study also found, among other things, that free riding isn't uniform across connection speeds. Although it's logical for users to free ride — uploading files is not only inconvenient but also yields no personal benefits — the authors say that developers must institute new protocols to limit free riding if Gnutella is to survive. Ironically, they add, doing so could cost Gnutella many users, who might move to P2P systems that lack such limits.

IEEE Intelligent Systems
www.computer.org/intelligent/
May/June 2005

"Identifying Interesting Visitors through Web Log Classification," by Jeffrey Xu Yu, Yuming Ou, Chengqi Zhang, and Shichao Zhang

Given the abundance of consumer sites on the Internet, standing out among

continued on p. 13

network architects more choices. Nonetheless, he says that even after standards are set, users seeking advanced features such as fast roaming or location tracking will have to get proprietary extensions.

July 2005

"RFID vs. Wi-Fi ID," by Andy Dornan

Radio frequency identification's popularity, and its close link to Wi-Fi, have led some developers to envision the creation of buildings with RFID readers embedded throughout their infrastructures. Several established companies, led by Cisco Systems, are

promoting Wi-Fi itself as a way to produce RFID-like applications. Start-up Reva Systems hasn't introduced any products yet, but it has announced a basic architecture for its Tag Acquisition Network, a system of RFID readers that would work with passive tags with ranges of just a few inches. Such networks could aid in managing inventory, but not monitoring movement in a room or building. To monitor movement, users would need a system with a longer reach — perhaps requiring active, battery-powered RFID tags, which would increase tag costs from pennies to dollars.

Programming and Development

JavaPro

www.ftponline.com/javapro/
Volume 9, Number 1

"Pushing Portal Potential,"

by David Hritz

Portal applications are becoming increasingly prevalent on the Internet primarily because they provide functionality for things like commerce, content management, searching, and collaboration. But Hritz says they owe some of their popularity to newness, which leads some buyers to opt for portals even though they pro-

vide more services than users actually need. He explains how to decide whether a portal application is necessary for a given user's needs or if a Web application will do. Among other things, Hritz discusses some important features, including customization, integration with legacy applications, and the Java community's efforts to define standards for developing "portlets," the subcomponents that make up portals, using Java specification request 168 (www.jcp.org).

Security

Network Magazine

www.networkmagazine.com

July 2005

"Adware Laws Get Teeth?"

by Andrew Conry-Murray

The US Congress is continuing to explore antispyware legislation. Pending bills include HR 29, which would make malicious software such as key-stroke loggers and browser hijackers illegal, and HF 744, which would require prison sentences and fines for those involved in spyware or phishing scams. Congress still hasn't decided how to address adware, but it's study-

ing the problem and at least one industry official believes this alone has pressured companies such as Claria and 180solutions to better inform users about potentially unwanted software.

"IPS Odyssey,"

by Andrew Conry-Murray

Conry-Murray suggests that today's malware and worm threats have "out-evolved" the abilities of most signature-based intrusion-prevention systems (IPSs). Although vendors can implement new signatures within hours, this window is still big enough for attackers

to enter systems. Consequently, he says, vendors in both the IPS and host-based IPS (HIPS) arenas are increasing efforts to shut that window of vulnerability. Conry-Murray outlines a new generation of “upstart” HIPS products that challenge the traditional premise that software can discern good and bad behavior. The products take various approaches, including preventing buffer overflows by enforcing essential programming conventions; generating protected subsystems to run untrustworthy programs without hurting hosts’ critical files; and creating strict enforcement agents that run only approved executables.

Web Services

JavaPro

www.ftponline.com/javapro/
Volume 9, Number 1

“Write a Web Service Server,”

by Kevin Jones

As with other aspects of software development, you can write a Web service server using more than one method. Jones acknowledges that the best approach is probably to first write the Web Services Description Language (WSDL) document and then generate the required code from that. However, he explains that starting with Java code presents a more accessible method given the programming community’s breadth of Java expertise; it also helps programmers better understand the “larger picture.” He outlines a method that, among other things, touches on how to interact with the remainder of the Web application, and describes faults and complex types.

XML

xmlPC Magazine

www.pcmag.com
9 Aug. 2005

“Flipping File Formats,”

by Sebastian Rupley

Elsewhere in the IEEE Computer Society

continued from p. 12

competitors is challenging at best. However, if consumer sites can find ways to increase customer loyalty, their chances of survival increase dramatically — research indicates that raising customer retention by as little as 5 percent can generate up to a 95 percent jump in profits. To help consumer sites better identify which purchasers are likely to return, the authors have developed a subjective classification technique using weblogs that provides firms with “actionable” customer patterns even with small data sets. Their approach roots out Web site visitors who are likely to purchase something using variables that include how much time customers spend on certain pages, how deep they navigate to lower-level pages, whether they use the HTTP POST mode, and whether they access images or graphics. The technique also includes sifting through the patterns of the search engines’ network robots.

IEEE Security & Privacy

www.computer/security/
May/June 2005

“Collaborative Internet Worm Containment,” by **Min Cai, Kai Hwang, Yu-Kwong Kwok, Shanshan Song, and Yu Chen**

To help contain Internet worms, a group of students and faculty from the University of Southern California is developing a prototype system (<http://gridsec.usc.edu>) to defend against distributed denial-of-

service attacks. Netshield is a fast, scalable security overlay network based on distributed hash tables; it not only detects intrusions but also exchanges alert information. The authors outline two components of the system, as well as experimental results from two large-scale simulations, one of which showed that deploying their collaborative WormShield monitors on just 1 percent of vulnerable edge networks let them detect worm signatures roughly 10 times faster than with independent monitors.

“RFID Privacy: An Overview of Problems and Proposed Solutions,” by **Simson L. Garfinkel, Ari Juels, and Ravi Pappu**

As radio frequency identification (RFID) inches closer to widespread use in the US marketplace, the privacy debate over how it might affect consumers continues unabated. The authors review the risks to both industry and individuals, from corporate espionage to Big Brother scenarios. They also outline many technical solutions — from “killing” the tags at the purchase point to encryption to blocking readers like you’d block spam. In addition, they cover possible regulations and guiding principles that could be considered in the future. Ultimately, they suggest that all of the solutions hinder RFID’s potential in some way, but they’re hopeful that the ongoing public debate will lead to a satisfactory security solution.

Microsoft Office 12, due out in late 2005, will include new royalty-free, XML-based open formats for Excel, Word, and Powerpoint. Unless users opt to revert to the current binary format, files created in those applications will save as .xlsx, .docx, and .pptx by default. The files will be saved as compressed files, including the underlying XML and offering better error recovery and storage.

Compatibility issues will certainly

arise when, for instance, a user with Office 2003 receives a newly formatted file. Microsoft says those users will be prompted to download a converter, and the company might let IT departments implement the converters in the same way it currently distributes its service packs to its registered users. □

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