

SECURITY

Correlation and Diamonds Used to Confound Intrusion

As hackers become ubiquitous—and sophisticated—they generally assume a lower profile than they have in the past, choosing to remain anonymous and gain money instead of notoriety, according to *Baseline* magazine. Joe Payne, president and chief operating officer at iDefense Security Intelligence Services, said that in contrast to the days when underground glory was the key motivator for a hacker, a successful attack today “is one that doesn’t get noticed.” These days, system pirates enjoy lucrative chests to raid, and the numbers just keep going up.

Hackers are now going for the cash, and they’re getting better at it.

A 2005 Computer Crime and Security Survey conducted by Computer Security Institute (CSI), in conjunction with the FBI’s Computer Intrusion Squad in San Francisco, said that losses of \$130.1 million were reported by 639 respondents. That’s over \$200,000 per incident. The figure is actually down from the previous year; however, losses per respondent soared in terms of proprietary information thefts, from \$168,529 in 2004, to \$355,552 in 2005, according to *Baseline*.

As an example of just how common system attacks are now, the CERT Coordination Center at Carnegie Mellon University’s Software Engineering Institute stopped counting the number of reports it received after 2003, when 137,529 serious incidents were tallied. Compare that number to six serious reports in 1988 and it is clear the battlefield has completely changed. Bank of America’s security chief identifies millions of threat “events” each month, and says most of them don’t get treated because they are relatively innocuous worms that remain outside the network. The University of Georgia IT security force claims it repels 80,000 to 90,000 events each day.

So how are IT professionals keeping up?

In addition to the classic firewalls between a company’s network and the public Internet, some security pros are moving toward “behavior-based” detection technologies, which set baseline activity levels on the network and then use various monitoring strategies to detect anomalous traffic patterns, such as heavy use during times when lighter volume is expected. These strategies are a response to so-called “zero-day” attacks, in which a breach is accompanied by an instantaneous strike that avoids signature recognition, allowing no time for system protectors to respond.

One such behavior-based security technology, called “correlation,” is a combination intrusion-detection/intrusion-prevention method that filters the millions of events encountered by businesses to identify and subdue an attacker. Correlation programs take pattern recognition to a

different level, basing their strategies on what their designers know about sophisticated hacking methods. For example, a fraudulent Web site might try to appropriate a bank’s graphics to construct a site that lures a victim into providing sensitive information like social security or account numbers. The hacker might enter a bank’s site, rip one graphic, then return hours later to rip another. The hacker might even come back the next day, knowing that three incidents in a 24-hour period normally would escape system monitors.

Taken as separate instances, these events might not cause alarm. But a correlation engine could filter and sort the data points and discover that the events happened at more than one company site, and that the actions were committed by the same IP address, for example.

Some major banks have been using NetForensics’ Open Security Platform security information and event

ACQUISITIONS

Siemens Makes Inroads in China

Reuters reported that German firm Siemens has signed a multi-million dollar deal to acquire PhotonicBridges, a Chinese company that develops optical transmissions systems equipment using a technology called synchronous digital hierarchy (SDH). Financial details were not available, but the purchase signals Siemens’s commitment to establishing its presence in China’s emerging high-tech manufacturing market.

A Siemens representative said that it will consolidate the Chinese company into its own operations once the deal is finalized. PhotonicBridges has approximately 300 employees, using its SDH technology to produce optical transmissions systems with ranges up to 125 miles.

The representative also revealed that Siemens is not stopping there, saying observers should expect a major deal in the next 12 to 24 months. Chinese media reports are speculating that the German firm is looking at Harbour Networks, a network equipment manufacturer that was founded by a former employee of China’s leading telecom products maker, Huawei Technologies.

In 2004, Harbour Networks considered a \$400 million IPO in Hong Kong, but backed off as the market’s favor for such deals waned. ■

planning management programs, one of the sophisticated and multileveled products that can correlate the massive amount of data seen by firewalls and detection schemes. Such products are designed to detect patterns that go unnoticed by other systems. Pitney Bowes uses products from several companies including McAfee for general vulnerability management, Lumeta for networks, and AppDetective for applications.

According to Daniel Minoli of *NetworkWorld* (<http://www.networkworld.com>), the greatest need in enterprise network systems is standardized security architecture that “should address administrative, communication, computer, radiation, personnel, and physical security.” In other words, companies must think about security as a defining component of their network’s configuration, construction, and operation.

Network builders conceive a company’s architecture based on the enterprise’s operational needs, and security architecture deserves the same level of attention to ensure that protection levels meet or exceed threat potential based on an organization’s type of business. Governments, for example, continuously struggle to stay a half-step ahead of hackers due to the sensitivity of the information they store and transmit.

Diamonds might turn out to be everyone’s best friend.

One of the most exciting innovations in ultra-high security is quantum cryptography that uses diamond-based optical fiber technology to achieve almost guaranteed secure data transmission over long distances. Proprietary manufacturing techniques actually grow individual diamond crystals on the tips of optical fibers. Synthetic diamonds, as opposed

to mined gems, have a flaw that emits a single photon that travels within the fibers to prevent eavesdropping, maintaining unheard of levels of security.

MagiQ, Qucor Pty Ltd., and California-based SGI—companies on the forefront of the technology—recently formed an A\$9 million partnership with the Australian government and Quantum Communications Victoria (QCV), a firm that claims to derive its “guaranteed” security from the laws of quantum physics. Dr. Shane Huntington, University of Melbourne scientist and CEO of QCV said in *NetworkWorld* that diamond-based quantum cryptography is “not a stronger form of encoding, it’s a new paradigm. So if someone steals the information, you definitely know it’s happened. If you’re sending one photon at a time and one goes missing you know it.” ■



YOUR SUCCESS IS OUR SUCCESS

Become a key player in enhancing business strategies through Information Technology (IT).

The Technology Programs offer professional Masters Degree and Certification both on-line and on-campus in:

- * Information Technology
- * Information Assurance
- * IT Service Management
- * Telecommunications Management

University of Dallas is designated as a Center of Academic Excellence (CAE) by the National Security Agency (NSA) of the Department of Defense (DoD) and Department of Homeland Security for the Information Assurance (IA) program.

To apply today or for more information:

Visit: www.thedallasmba.com or

Contact: Mihir Mistry,

Director of Technology Programs

Email: mmistry@gsm.udallas.edu

Phone: 972-721-4091

SOFTWARE

Sun to Open-Source Java

Sun Microsystems has decided to finally open-source its Java programming language. Programmers have long clamored for Sun to open-source Java, but company executives always resisted because of compatibility concerns and control issues.

Sun's hope is that open-sourced Java will increase its business by increasing the language's versatility, availability, and exposure, in addition to broadening the company's avail-

able revenue streams. No timeline has been set for the launch of open-source Java.

Sun rivals and Java users alike think that the open-source code will lead to more innovation. For example, although IBM is a competitor, it is willing to help the process because of its involvement with Java, said Rod Smith, IBM's vice president of emerging technology. He said that Java's popularity has outpaced its innovative capabilities because of Sun's reluc-

tance to open-source it.

Sun will not make Java's source code available immediately, but did announce that programmers will have access to other programs including Sun Java Studio Creator, Sun Java System Portal Server, Sun's Java Message System-based message queue, and Web Services Interoperability Technology. This follows the company's launch last year of OpenSolaris, an open-source addition to its Solaris operating system. ■

Microsoft Gets Enterprising with New Searchware

According to *Infoworld*, Microsoft is reviving its voyage into enterprise search with the unveiling of its new search tool, Office SharePoint Server 2007. Microsoft has adapted the program to focus more on search than the software's previous version, SharePoint Portal Server 2003, which primarily was a Web portal builder and document sharer. The new version, which will be available to customers in Microsoft's next office suite, Office 2007, will have capabilities intended to respond to Google's innovations in the enterprise search realm.

Enterprise searches currently benefit from a Google functionality that, with some additional software, allows companies to search data in systems from Cisco Systems, Oracle, and others. Google has been offering firms these kinds of customizable search options for some time, and now Microsoft wants a bigger chunk of the market. Microsoft said its enterprise product will enable companies to deeply mine employees' searches to create interest-based information structures, and will also reduce employees' search time because they will more easily be able to access other workers' knowledge.

In an April *Infoworld* article, Dave Girouard, Google's vice president and general manager for enterprise business, said that vendors need to

make their enterprise search software as user-friendly to employees as their standard search engines are to consumers. ■

EMPLOYMENT

IT Services Giant TCS Continues Hiring Spree

According to *ZDNet*, information technology services provider Tata Consultancy Services (TCS) will add 30,000 new jobs in the next fiscal year, bringing its roster to over 62,000 employees in 34 countries. TCS hired 10,000 people in 2004, had 45,714 employees in March 2005, and is now India's largest technology services company.

TCS reported that net income for fiscal 2006 leaped to \$649.2 million, with revenue of nearly \$3 billion, an increase of over 36 percent from the previous year when 21,140 jobs were added. If the firm meets next year's hiring goal it will mark a 44 percent increase over the actual number of employees hired last year. Most new workers at TCS will continue to be hired directly out of Indian schools, with college graduates starting at 250,000 to 350,000 rupees per year, which equals about \$6,000 to \$9,000 US.

Girija Pande, the company's Asia-Pacific regional director, said that his territory's growth is consistent with that of the entire firm, and that TCS wants to expand into China in the next five years, hoping to grow its numbers from 400 to almost 6,000. Other projects planned in the region include a joint venture with Microsoft to begin operations in Beijing in June, and a Singapore-based banking technologies center to open in July. ■

STANDARDS

Microsoft Rolls Out Anticipated Vista Specs on Web

According to *InfoWeek*, Microsoft has finally revealed the system requirements needed to run its forthcoming Windows Vista operating system. The software giant placed specs under two different labels: “Vista Capable” and “Vista Premium Ready,” on a special Vista-dedicated section of its Web site called “Get Ready.” Customers can find information there that explains what they will need to run the bare-necessities version of the OS, and the option-loaded version, respectively.

Microsoft might be using a marketing strategy for its dual-option OS that resembles the Apple pricing structure, which is essentially a three-tiered system that keeps choices simple while clearly telling customers what they are getting for their money. As a result, the Macintosh avoids the option-laden mayhem that often confronts a PC purchaser, especially at big-box retailers where models can number in the hundreds.

Some of the requirements to run Vista at the “Capable” level are an

800MHz or faster processor, 512 Mbytes of memory, and a Direct X9-capable graphics processor.

But customers who want to run the “Premium Ready” version will need significantly more: a minimum 1 Gbyte, 32- or 64-bit processor, 1 Gbyte of RAM, 128 Mbytes of graphics room, at least 15 Gbytes free on a 40-Gbyte hard drive, and a DVD-ROM drive.

The specs have been widely anticipated by PC manufacturers who have waited to see exactly what kinds of machines they’ll want to produce. Those firms received some unkind news recently when Microsoft announced that Vista’s release would be delayed until January 2007. They had hoped to slap the “Vista” stickers Microsoft provided onto boxes rolled out in 2006’s fourth quarter. Attempting to buoy spirits, Microsoft vice president of Windows product management, Mike Sievert said, “Customers now have the information they need to get a great Windows XP-based PC today that will deliver rich Windows Vista experiences tomorrow.”

But some users aren’t so sure. One beta-tester expressed doubts about whether his current system will be able to run the version of Vista he wants, and bristled at the thought of purchasing an entirely new set-up—one that may not even run the new OS optimally.

Michael Cherry, an analyst with Kirkland, Wash.-based Directions on Microsoft, was quoted in *InfoWeek* as saying, “I don’t want my computer purchase to be as complicated as buying a car, but I still think Microsoft is making it hard to answer what should be a relatively easy question.” Cherry said that he will wait until Vista hits the market before sinking money into a new system, and advised other consumers to do the same. ■

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 IT Professional Magazine*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; (714) 821-8380; fax (714) 821-4010. Email: manderson@computer.org.

NETWORK ENGINEER. Analyze, design & develop comp system ntwrks using routing techniques including TCP/IP, HTTP, DNS, SMTP, FTP, & NetBIOS & IP address mngmnt systems in UNIX & Windows NT systems. Dsgn & implement firewalls using Cisco PIX & Routers, Check Point, Netscreen, & ISS. Monitor ntwrk ops & dvlp monthly reports including log file analysis, utilization reports, & vulnerability & incidence analyses using ISS Real Source & Scanners, Cisco, Axent, & nmap. Req: Master’s in Comp. Sci., Comp. Info. Sci., or Comp. Eng. or Bachelor’s in Comp.Sci., Comp. Info. Systems, or Comp Eng. & 5 yrs exp., 40 hr/wk. Job/Interview Site: Brea, CA. Email resume to ntwkjobs@nisum.com or mail @ 2500 E. Imperial Hwy, Ste 201-317, Brea, CA 92821.

SOFTWARE CONSULTANT (Garner NC) for Sigma Electric Mftg, to design, implement and analyze ERP systems; provide support/maintenance for PeopleSoft/JD Edwards and RF Smart Bar code system.

Req’s Bach + 2 yrs exp, which must inc AS400. Send resume to jobs@sigmaelectric.com or W. Jackson, 120 Sigma Dr. Garner 27529.

PROGRAMMER ANALYST. Dsgn, dvlp, mntn & cstmr sftwr apps in Microsoft Visual Studio platform using ASP.NET, VB.NET, XML, JAVASCRIPT & SQL Server. Test apps for perform, data integrity & validation issues. Plan, dsn & dvlp custom interfaces between apps. Req: Bach in Comp Sci, Comp Info Sys., Comp Eng, or Electrical Eng. 40 hr/wk. Job/Interview Site: Ventura, CA. Fax Resume to: Computer Design and Information Services @ (805) 477-7529.

CATHAY MORTGAGE LENDING CORP in Orlando, FL needs a Data Analyst to design/implement/maintain database and analyzes financial data. Bachelor’s degree in CS, MIS or related field. Competitive salary. Fax resume to 407-898-0037.

WIRELESS TECHNOLOGY

Linksys Ships New Wireless IP Phones

Linksys, a division of Cisco Systems, is introducing its WIP 300 and WIP 330 wireless phones, according to *TMCnet*. The two models are the first in a line of phones that use VoIP technology, which allows users to make calls over 802.11 wireless networks.

In addition to their compliance with IEEE 802.11b/g standards, both mod-

els have large, color LCD displays, user-friendly interfaces that enable quick configuration for Wireless-G connection, and a built-in browser that can access web-based email, view web sites, and accept some Internet-based video. The phones can also connect with public "hotspots," and access a Linksys wireless router apparently with two-touch operation.

The WIP 300 and WIP 330 phones will retail for about \$220, and \$370, respectively. To complement the releases, Linksys recently introduced its Network Optimizer for VoIP and gaming, which prioritizes network data streams to make games run more smoothly and improve the quality of VoIP calls. ■



Here now from the
IEEE Computer Society

IEEE ReadyNotes

Looking for accessible tutorials on software development, project management, and emerging technologies? Then have a look at ReadyNotes, another new product from the IEEE Computer Society.

ReadyNotes are guidebooks that serve as quick-start references for busy computing professionals.

Available as immediately downloadable PDFs (with a credit card purchase), ReadyNotes sell for \$19 or less.
www.computer.org/ReadyNotes

