Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 32
7 Ιουλίου 2006

New Method Better Predicts Software Vulnerabilities
Colorado State University (06/28/06)

Researchers at Colorado State University are studying the process of discovering vulnerabilities in operating systems and major software applications in an effort to better predict the number and severity of vulnerabilities that are likely to arise in the near future. The complementary method employed by Y. Malaiya, a professor in CSU's Computer Science Department, and doctoral student O. Alhazmi consists of modeling the vulnerability detection rate with the Alhazmi-Malaiya Logistic model and based on the developer, predicting the number of vulnerabilities per 1,000 lines of code. The approach would help give developers and companies a better indication of when and how many patches they will need to develop for applications and systems by a certain time, and before hackers have an opportunity to exploit them. For example, the Alhazmi-Malaiya Logistic model predicted last year that Windows XP would have a rapid growth in vulnerabilities, which have now risen to 173 from 88 in January 2005, and it was just as accurate in determining that there would be few new vulnerabilities for Red Hat Linux 6.2, which has been unchanged at 117. "The hope is that a vulnerability gets patched before it gets exploited," says Malaiya.

Critic: Paper Vote Records Vital
Miami Herald (06/28/06), S. Benn

Stanford University computer science professor D. Dill told two Florida groups that their state is behind the curve in having a system of paper records to verify electronic votes during a lecture in Coral Gables. Dill, an e-voting expert, told members of the Miami-Dade Election Reform Coalition and the Human Services Coalition that 27 states have passed laws that require votes from e-voting machines to be verified by paper records. Dill helped create the Verified Voting Foundation, which has found flaws in Diebold touch-screen voting machines that would enable a hacker to manipulate election results. Touch-screen voting machines must allow for independent verification of votes to ensure accuracy of results, said Dill, who added that his group is working with government officials to improve the voting process so that counties use "the best practices for running elections." Dill said more citizens need to get involved in monitoring the e-voting process. "You can have the most transparent system in the world, but unless you have people looking into that transparent system, you're not going to have the trust of the voter," he said. After the lecture, Dill took questions from the audience, including one about the possibility of Internet voting, but he said it was unlikely unless there are a number of breakthroughs that could ensure votes were trustworthy.

Human Trails in Cyberspace
Chronicle of Higher Education (06/30/06) Vol. 52, No. 43, P. A18; J. Young

Techniques for mapping online activity and the challenge of drawing insightful conclusions from this information were detailed by a panel of academic and industry experts at a University of Pennsylvania conference titled "The Hyperlinked Society." University of Michigan professor L. Adamic demonstrated a map of connections between political bloggers at the

start of the 2004 US presidential election, which was used to determine whether blogging activity corresponded to preconceived notions about conservatives and liberals' offline behavior. Adamic says conservatives were more interlinked than liberals, but not by a wide margin, while both sides were virtually tied in terms of blogging activity. The distribution of political blogs in visual space is a reflection of the frequency of their links, which also holds true for a map of over 1,000 popular blogs created by Matthew Hurst of Nielsen BuzzMetrics. Hurst's map indicates the number of links to the blogs, the type of blog software in use, and what type of server hosts the sites; according to the map, the blogs with the most links cover technology and social-political commentary, which helps Nielsen BuzzMetrics give clients advice on tapping the Internet. The goal of Microsoft Research's Netscan project is to make online community dynamics more comprehensible through the analysis of behavior on the Usenet online discussion forum. "What we're trying to do is show patterns of contribution to threaded conversation communities," explains M. Smith, who helms Microsoft Research's Community Technologies group. Smith and colleagues have invented a method to outline a user profile by studying data maps of their posting behavior rather than the content of their messages.

Hacker Attacks Hitting Pentagon
Baltimore Sun (07/02/06) P. A1; S. Gorman

While the reported number of attempts to breach the Pentagon's computer networks has spiked from fewer than 800 in 1996 to more than 160,000 last year, the government's efforts to shore up its cybersecurity defenses have stalled. An initiative undertaken by the National Security Agency to encrypt sensitive information and restrict access at the Defense Department and other government bodies is seven years behind schedule, due partially to fundamental differences between the two agencies. According to an internal NSA report, 30% of the agency's security equipment provides insufficient protection, and 46% of the equipment is nearing that status. "Much of the existing cryptographic equipment is based on ... technologies that are 20-30-plus years old," according to the report, which also noted the sharp increase in the sophistication of cyber criminals. A security team spent weeks addressing a recent incident where Chinese hackers gained access to a computer system that serves the Joint Chiefs of Staff, according to two sources close to the incident. "This stuff is enormously important," said John Stenbit, who served as the Pentagon's CIO until 2004. "If the keys get into the wrong hands, all kinds of bad things happen. You don't want to just let a hacker grab the key as it's going through the Internet." The Pentagon reports that attacks against its computers have increased 200-fold in the past decade, citing growing threats from individuals, terrorist groups, and foreign states. In a recent court case, two men were charged in Miami with hacking into government computers and sending military secrets to China. Iran has also emerged as a major threat to the government's aging computer systems. The NSA is developing the Key Management Infrastructure program to strengthen the government's defenses, though it has been impeded by high costs and poor management.

Securing Europe's Future Information Society
IST Results (07/05/06)

In an effort to combat the mounting security risks associated with Internet services and commerce, the EU has launched an effort to shore up the reliability of its networked systems. Drawing on Europe's leading security experts, the SecurIST project is formulating a roadmap for the continued improvement of network dependability and security throughout the continent. Security, which includes confidentiality, integrity, and accessibility of information, is closely related to dependability, which encompasses reliability, safety, and maintainability in

the face of intentional and accidental threats. "The project should provide Europe with a clear European-level view of the strategic opportunities, strengths, weakness(es), and threats in the area of security and dependability," said Jim Clarke, coordinator of the SecurIST program. "It will identify priorities for Europe and mechanisms to effectively focus efforts on those priorities, identifying instruments for delivering on those priorities and a coherent time frame for delivery." The program created a security taskforce by dividing its focus into different linked areas such as security policy, application security, identity and privacy, and biometrics. An advisory board helped the more than 200 SecurIST researchers develop a series of recommendations, including enhancing the centralized control mechanisms and empowering individual users to guard against identity theft and other cyberthreats. The researchers have identified service oriented architecture as a key priority for secure software design, as well as the development of the broad disciplines that enable security: cryptology and trusted computing.

Researchers Claim Great Firewall Workaround
IDG News Service (07/05/06), S. Lemon; N. Gohring

Researchers from the University of Cambridge have reported the discovery of a method for working around the Chinese government's complex Internet filtering system, though some question how much of a breakthrough their research really is. The filtering system uses routers and intrusion-detection applications to screen for keywords within packets of Internet transmissions. A request for Web sites that include prohibited words such as "falun" is blocked by sending reset (RST) packets to the client computer and the Web server, severing the connection between the two. The Great Firewall keeps the connection broken for a period of time that averages around 20 minutes, but can last up to an hour, a finding that some researchers say was already common knowledge to those familiar with the system. "There's nothing in there I didn't know two years ago," said M. Robinson, an IT expert in Beijing. "The connection reset system described in the paper is only one layer of a much larger multilayer content control system. Using encrypted proxy servers is the only way around all of them." The researchers suggested special software that could ignore the RST packets as a potential workaround to the Great Firewall, though Robinson counters that creating a proxy connection involves the same amount of work and provides a more complete solution. R. Clayton, one of the Cambridge researchers, counters that the link to proxies is generally unencrypted so that Internet traffic is still subject to censorship. Clayton hopes that software companies such as Microsoft will begin creating TCP/IP stacks that ignore the resets to increase security.

Wariness of U.S. Tech Lag on the Rise
United Press International (06/26/06), A. Darm

Integrating technology into every public institution is critical to the United States' competitiveness in the 21st century, according to experts speaking at a conference hosted by the New America Foundation on Capitol Hill. Technology education has the capacity to broaden access to information at virtually every national institution. "Acquiring the best technology for learning is not a problem but a challenge; it is an opportunity to excel," said D. Fletcher of the Institute for Defense Analyses. Technology education is particularly valuable because the computing experience is highly personal and interactive, according to H. Kelly, president of the Federation of American Scientists. Speakers also emphasized the value that technology education has for children, especially since the average child spends six hours each day using electronic media, according to M. Calabrese, director of the Wireless Future program at the New America Foundation. Lawmakers are working to pass the Digital Opportunity Invest-

ment Trust (DO-IT), legislation that would support technology education through programs such as Immune Attack, an educational video game about human immunology. Digital Promise's Rayne Guilford likened the scope of the legislation to the GI Bill and the Northwest Ordinance. "Once a century, Congress makes a major investment in transforming training and education," Guilford said. "The Digital Promise is the 21st century equivalent of the GI Bill." The absence of a commercial market is a central impediment to the DO-IT initiative, though some private corporations are realizing that technology education is critical to preserving the United States' climate of innovation.

Wider Authority Urged for IT Managers
Federal Times (06/26/06) Vol. 42, No. 21, P. 8; A. Curl

Security experts told lawmakers that Congress should give federal CIOs and chief information security officers (CISOs) more power to prevent more security breaches from occurring such as the one at the Veterans Affairs and Agriculture departments. They also said information officers at government agencies need to have more authority to guarantee compliance of data security guidelines. E. Spafford at Purdue University's Center for Education and Research in Information Assurance and Security said CIOs and CISOs need sufficient funding and a trained staff to perform an effective security plan. A laptop containing the personal information of 26.5 million veterans was stolen from a VA employee's home last month and the Agriculture Department's computer systems, which stored 26,000 current and former employees' information, was recently hacked. Spafford, along with former VA CISO B. Brody, told the committee there is a need for someone else besides the VA to enforce privacy polices. Brody testified before the House Veterans Affairs Committee with other experts on June 22. "We've found that individual directors often feel they can override policy when it gets in their way," said Spafford. "Unfortunately, the people making these decisions don't have the training to understand the consequences."

New Research Center to Combat Identity Theft
TechNewsWorld (06/29/06), E. Morphy

A new group called the Center for Identity Management and Information Protection has been formed to fight identity theft and data losses that have occurred at colleges, in the private sector, and the government. The group will be based at Utica College in New York and will focus on how to prevent and detect identity fraud and theft, how to spot cybercriminals, how to improve identity authentication systems, and how technology can protect and share information. Experts agree that establishing the Center is a step in the right direction. "Most of the incidents of identity theft lately, at least anecdotally, have been cases of employees taking home laptops with sensitive information on them that were subsequently stolen," says R. O'Brien, senior security consultant at Sophos. The Center will be led by G. Gordon, a professor at Utica College, while the board of advisors of the college's Economic Crime Institute will oversee the Center's research. In addition to Utica College, the Center was founded by LexisNexis, IBM, the United States Secret Service, the FBI, Carnegie Mellon University Software Engineering Institute's CERT/CC, Indiana University's Center for Applied Cybersecurity Research, and Syracuse University's CASE Center. The Bureau of Justice Assistance, Office of Justice Programs, and Utica College's CIMIP will team up for the Center's first project, which will look at existing and upcoming criminal identity theft groups.

A Culture of 'No'
InformationWeek (06/26/06)No. 1095, P. 23; T. Claburn; E. Whiting; E. Malykhina

IT professionals must take a paternal, security-minded view toward employees' take-up of popular, often free consumer-oriented Web tools, but not at the expense of innovation, which is essential to companies' ability to rapidly adapt to change. There is a growing paranoia about security among business technologists in light of much publicized system intrusions, vulnerabilities, and advisories about shady employee conduct. However, "if [IT teams] put policies in place and make it so that people go around them, they end up opening up bigger security holes," warns Gartner VP D. Smith. One strategy to help ensure continued innovation while giving employees sufficient maneuverability is for companies to collaborate with vendors to make popular applications secure. Cox New England's B. Shipp recommends that companies try to understand the value of rogue apps, which obviously fulfill some need beyond the capabilities of IT; "They're all red flags, but they're also opportunities for doing something better," he maintains. Google Enterprise general manager D. Girouard said at the recent MIT Sloan CIO Symposium that companies must broaden their menu of options in order to maximize the productivity of innovative workers. ProBusiness Services network engineer B. Pierce does not endorse unconditional employee usage of rogue apps, suggesting that imported items should be subjected to security checks, while any output from the unauthorized software must exhibit compatibility with corporate software standards. "Does IT Matter?" author N. Carr believes workplace-based consumer technology will trigger an increase in internal IT needs in the short term because data control and integration across Web applications requires on-staff expertise, but he predicts that most corporate IT positions will be phased out over the next 10 years.