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

Δελτίο 22
29 Απρίλη 2006

Congress Readies New Digital Copyright Bill
CNet (04/23/06) McCullagh, Declan

Despite several years of pressure from technology companies and academics to moderate the provisions of the Digital Millennium Copyright Act (DMCA), Congress is poised to move in the other direction with an expansion of the bill's prohibitions against software that evades copy protections. Major copyright holders such as the Recording Industry Association of America have already voiced support for the draft legislation, which also expands the wiretapping and enforcement powers of federal police. The proposed legislation, drafted by the Bush administration and supported by Rep. L. Smith (R-Texas), would create the new federal crime of intentionally bypassing copyright protections that would be punishable, regardless if the piracy was successful or not, by up to 10 years in prison. A bill calling for the scaling back of the DMCA restrictions in the name of fair use has been tied up in committee since being introduced by Rep. R. Boucher (D-Va.) in 2002. The draft legislation broadens the scope of Section 1201 of the DMCA that currently bars only the trafficking and distribution of copyright-circumvention software or hardware by making it unlawful for anyone to "make, import, export, obtain control of, or possess" any such tools that could be redistributed. Critics have issued a report charging the DMCA with stifling free speech and innovation. The draft legislation also authorizes wiretapping in copyright crime investigations, criminal prosecution of infringement on works not registered with the US Copyright Office, and stiffer penalties for criminal infringement than prescribed in the 1997 No Electronic Theft Act.

Linux Desktop Growth Could Spur New Malware Activity
Computerworld (04/20/06) Lai, Eric

As Linux is implemented as a desktop OS in a growing number of organizations and institutions, including the Indiana Department of Education, experts say the platform could become increasingly targeted by malware. Right now, one of the main attractions of Linux is its relative immunity from malware as compared to Windows. However, the emergence of the cross-platform proof-of-concept virus Virus.Linux.Bi.a/Virus.Win32.Bi.a has raised concerns that actual malware will be launched inevitably. "I think we'll see an increase in virus activity as Linux becomes more mainstream," says J. Ulrich of The SANS Institute. The addition of new access controls to the upcoming Windows Vista may also push some virus creators to target other OS platforms, although Red Hat and Novell say they have enhanced their own access controls in their respective offerings Security Enhanced Linux and AppArmor.

Danger: Authenticating Email Can Break It
CNet (04/19/06), J. Evers

Email authentication schemes such as SenderID and DomainKeys Identified Mail (DKIM) have drawn attention as ways to guarantee email senders' identities, but experts warn that improper implementation could simply break an email system. Microsoft, the biggest backer of the Sender ID system, says the number of Fortune 500 companies that sent authenticated mail was up to 20% at the end of March from just 7% in July 2005. SenderID has seen more

adoption so far than DKIM, but it relies on ISPs, companies, and other Internet domain holders to identify their mail servers with published Sender Policy Framework (SPF) records. Meanwhile, Yahoo! and Cisco Systems are backing DKIM, which uses public-key cryptography to attach digital signatures to outgoing email. While the SenderID concept usually does not require companies to put new hardware or software into place, it does require them to do inventories of all their mail servers and to keep their records up-to-date, which can produce onerous IT costs. "If you are a large multinational organization, you may have email gateways in 10 countries, you may have marketing companies that send email on your behalf," said Paul Judge of the email security company CipherTrust. This complexity was a big problem at Bank of America, whose E. Johnson warned at the Authentication Summit in Chicago that companies must "deploy smart" to keep from breaking their email systems.

Council Releases Blueprint for Federal Cybersecurity Research
GovExec.com (04/25/06), D. Pulliam

A presidential advisory council has released guidelines for coordinating cybersecurity research and development among different federal agencies. Released last week by the National Science and Technology Council, the Federal Plan for Cyber Security and Information Assurance Research and Development involved members of more than 20 federal entities. The plan calls for the creation of standard cybersecurity metrics and other measures to inform researchers of the government's priorities, said S. Szykman, director of the National Coordination Office for Networking and Information Technology Research and Development. While the blueprint was developed solely by government officials, true coordination will be an ongoing effort that will include public comments and workshops to provide a forum for the private sector. "Certainly having a plan is one thing and executing it is another," said Szykman. "This group of people was focused on the [research and development] issues and understanding the existing issues and the priorities." The document is notable for its call for metrics and its emphasis on emerging technologies and incorporating security at the beginning of any deployment, though it is remiss in not defining how recipients of federal funding are to be held accountable, said A. Paller, research director of the SANS Institute. "Researchers are going to look at this as justification for anything they want to do," said Paller. Gartner's J. Pescatore says the blueprint should have identified specific areas where the government could fill in the gaps in research and development left by the market.

Robo-Ethics
Albany Times Union (NY) (04/21/06), M. Lisi

The fear that robots will eventually appear in surveillance systems and computer networks to monitor every element of human activity is a pressing concern for C. MacMurtie, artistic director of Amorphic Robot Works. "I am frightened to death of the way technology controls our society and is used against us," he said. "Technology can be a wonderful tool, and at the same time it's a very controlling tool. (Robotics) will continue to be used to give us luxury, and to repress us." MacMurtie was scheduled to deliver a keynote address at the Schenectady Museum's High Voltage Fields symposium on Sat. April 21 entitled "How Robotics Affects Our Society and Why It Concerns Me." MacMurtie worries that, just as in the movie "I, Robot," humans will instinctively create robots to perform undesirable tasks and endow them with human-like qualities. This year's symposium is thematically centered on the ethics of robotics to reflect the convergence of art and technology. The panel discussion will take up the issue of whether robots already play too much of a role in people's lives. The museum is also preparing a June exhibit entitled "Robots Rock!," featuring an ensemble of self-playing

robotic musical instruments. That sort of application for robotics is less concerning to MacMurtie, who acknowledges the field's many productive uses, such as space exploration and powerful computers. He is more concerned with the government's use of technology as an instrument of oppression in the post-9/11 age. "The really important thing to keep in mind is as our government is protecting us from terrorism, they've locked us down and used technology as the tool to lock us down with," he said. "The question is what (our government) has up its sleeve at this point. The stuff that's not out there is always more interesting than the stuff that's out there."

Software Insecurity: Plenty of Blame to Go Around
Government Computer News (04/18/06), W. Jackson

Attendees at the recent International Conference of Network Security were unable to agree about who should shoulder the blame for the persistent unreliability of software. Eset Chief Research Officer Andrew Lee attributed the poor quality to the barrier between developers and users, noting that an application that may seem perfectly intuitive to a developer can be put to illogical and destructive ends in the hands of a user. Lee also said most software is too complex to ever receive sufficient testing. Careful deployment could minimize disruptions caused by even the most flawed software, said Lockheed Martin's Eric Cole. "In a lot of cases, even though the bugs are still there, the impact to your organization can be mitigated" with a suitably architected and well-protected network, just as perfectly coded software is still vulnerable if improperly deployed, he explained. In response to an audience member's charge that organizations are more concerned with clever workarounds than with methodologies for solving problems, S. Katzke of the National Institute of Standards and Technology (NIST) said his organization could help, noting that the same level of due diligence created by the documents prepared for government users under the Federal Information Security Management Act (FISMA) could also apply to private industry. "The framework that we have established for federal agencies is really applicable to any environment," Katzke said. Participants also debated the relative worth of the Common Criteria program maintained by NIST and the NSA. Supporters claimed that the program enables a comparison between products, while critics charged that it is more about red tape than software quality.

Your Thoughts Are Your Password
Wired News (04/27/06), L. Sandhana

Researchers at Carleton University in Ottawa, Canada, believe it may be possible to observe a brain signal that is encoded with thousands of bits of information in a repeatable manner. Julie Thorpe, Anil Somayaji, and Adrian Chan are pursuing the idea of developing a system that would enable people to log on by thinking "yes" or "no" to a "pass thought," such as the memory of a birthday, or a predetermined song, picture, or video clip. The biometric security tool would monitor the individual's brain activity, and unlike other biometric security devices, would also allow people to change their pass code occasionally. The project builds on the research of those working to develop a brain-computer interface (BCI) that would allow prosthetic devices to read the brain-wave signals of people who are disabled. The project has its doubters in Iead Rezek, of the Pattern Analysis Research Group at the University of Oxford, and Jacques Vidal, a BCI expert in the computer science department of UCLA. Rezek says picking up signals would be "akin to recognizing speakers from muffled voices because, for example, the speakers are some distance away." Vidal contends that "the link between thought and brain waves is immensely indirect." The Carleton researchers face other challenges, including designing a system that is able to recognize the changes in the signature of a

pass thought over time, and making it more convenient to transmit brain signals without having to wear an EEG (electroencephalogram) cap, smeared with conductive gel, on the head.

New Software Protects Confidentiality of Data While Enabling Access and Sharing
Penn State Live (04/27/06), M. Hopkins, C. DuBois

Researchers at Penn State have developed new software called the Privacy-preserving Access Control Toolkit (PACT) that enables databases to communicate with one another automatically without compromising the security of the data and metadata. The software acts like a filter but is protected from eavesdropping and other attacks because the queries and other information are encrypted. PACT could prove to be beneficial to organizations such as government agencies, non-profits, and corporations, which frequently need to access data belonging to other organizations. Sharing data is normally difficult for these organizations because databases are usually constructed using different terms or vocabularies. As a result, organizations have to develop special-purpose applications in order to share data. But these applications must also address security, since organizations need to protect sources, intellectual property, and competitive advantages. These applications are often time consuming to develop, and are expensive since they have limited use. But PACT is more generic--which means that it can be applied to a wide range of scenarios, said Prasenjit Mitra, assistant professor of information sciences and technology at Penn State and a member of the research team that developed the software. In addition, researchers note that PACT is the first software to provide a framework that protects metadata while enabling "semantic operation" or sharing of information. Results from the researchers' experiments also demonstrate that PACT can be easily extended to large database systems in practical locations, Mitra said.

An Antiphishing Strategy Based on Visual Similarity Assessment
Internet Computing (04/06), Vol. 10, No. 2, P. 58, W. Liu, X. Deng, G. Huang

City University of Hong Kong researchers propose an antiphishing strategy that identifies potential phishing sites and evaluates suspicious pages' resemblance to actual sites registered with the system through visual cues. The SiteWatcher system employs two sequential processes: The first process runs on local email servers and watches emails for specific keywords and questionable URLs, and then the second process matches the potential phishing pages against actual pages and determines visual similarity by focusing on key regions, page layouts, and overall styles. SiteWatcher sends a phishing report to the customer if the visual similarity between the Web pages exceeds the corresponding threshold. The system represents block-level similarity as the weighted average of the visual similarities of all matched-block pairs between two pages. Layout similarity is defined as the proportion of the weighted number of matched blocks to the number of total blocks in the true page, and this similarity is measured by identifying a few blocks with identical contents and then matching other blocks based on the spatial relations of all blocks on the page via the neighbourhood relationship model; two blocks are considered to be matches if both bear a high visual resemblance to one another and fulfill the same position constraints with corresponding already-matched blocks. The similarity in overall style between two pages is defined as the correlation coefficient of the pages' histograms of the style feature values. The researchers built a prototype SiteWatcher system whose results showed promise, and they are currently focusing on making the system more efficient and weighing the possibility of deploying commercial applications. The researchers believe the SiteWatcher strategy could be a component of a larger enterprise antiphishing solution.