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

Δελτίο 57
18 Γενάρη 2007

Daylight Sought for Data Mining
Washington Post (01/11/07) P. D3; E. Nakashima; A. Klein

A Senate bill introduced on Jan. 10 would require that government agencies inform Congress about government data-mining efforts intended to "discover predictive or anomalous patterns indicating criminal or terrorist activity." Similar bills in recent years were not successful in the Republican-controlled Congress, but new Senate Judiciary Committee Chairman P. Leahy (D-Vt.), who co-sponsored the bill introduced by Sens. R. Feingold (D-Wis.) and J. Sununu (R-N.H.), has said that this Congress will assume an aggressive stance in the oversight of surveillance and data-mining programs. Leahy said, "The American people have neither the assurance that these massive data banks will make us safer, nor the confidence that their privacy rights will be protected." According to Leahy, over 52 federal agencies utilize data-mining, totaling 199 programs in all, although this number does not include NSA programs, since the agency will not reveal such information. Claiming that 300,000 names appear on the government's terrorist watch-list, including infants and members of Congress, Leahy said, "We also need to understand that a mistake in a government database could cost a person his or her job, sacrifice their liberty, and wreak havoc on their life and reputation." Predictive data-mining is becoming more popular, although Cato Institute director of information policy studies Jim Harper says the technique is not effective in finding terrorists, since there are not enough established "terrorist patterns" to build a model around. Privacy advocacy groups agree that data-mining has shown little evidence of its effectiveness, but the Center for Advanced Studies in Science and Technology Policy claims that while the system is not perfect, properly conducted oversight can make the necessary adjustments.

Computer Security: Adapt or Die
Computerworld (01/08/07), G. Anthes

Intel researchers are developing adaptive and resilient computing security technology that enables computers to communicate with each other concerning network activity in order to find a way to stay ahead of network attackers. Older security applications that rely on signatures are no longer a sufficient means of protection, as they cannot be updated as fast as new malicious content can be released. BT research engineer R. Ghanea-Hercock says, "For cutting-edge day-to-day protection, you'll have to have adaptive things that monitor what's happening on the network in real time." "Anomaly detectors" at local nodes are being developed by Intel to monitor for evidence of worms, such as a sudden increase in activity. If such an indicator is noticed, a computer will "discuss" the probability that the network is under attack with other machines, and if enough machines on the network agree on the attack, defensive measures would be taken. Recent changes to malware has slowed it down, allowing it to slip past traditional intrusion detectors that monitor for anomalous activity. Florida Institute of Technology computer science professor R. Ford says high-profile, massive attacks are being replaced by more secretive, "high value" exploits. He says, "That dramatically changes the threat profile." The Intel prototype, called Distributed Detection and Interference (DDI), is based on the idea that one computer noticing an increase in connections could mean a simple fluctuation, but 50 computers noticing even a slight increase in traffic most likely indicates

an attack. As adaptive security makes its way into the commercial world, the biggest threat to the technology's success are false positives, which can cause inconvenience or even lead users to ignore actual threats.

How to Leak a Secret and Not Get Caught
New Scientist (01/12/07), P. Marks

Open-source software engineers and political activists are believed to be behind a new online service that will allow anonymous users to post documents about the unethical actions of companies and governments without being traced. WikiLeaks will use the anonymizing protocol Tor (The Onion Router) to allow a network of servers to use cryptography to cover the tracks of data packets. The software the unidentified participants are testing is similar to the open-source software that powers Wikipedia. "Imagine a large room jammed full of people in which many of them are passing around envelopes," cryptographer B. Schneier says of Tor. "How would you know where any of them started?" The group will leave it up to site users to scrutinize and comment on any posted information to determine its validity. There are some doubts about the protection Tor offers, considering it has been breached by cryptographers in the past. Tor has been improved, but there is the risk that other breaches will occur. WikiLeaks could be up and running for the public by February.

Of Cyber Wars and Turf Wars
National Journal (01/06/07) Vol. 39, No. 1, P. 38; B. Swindell

As the 110th Congress begins its first session, federal data-security standards are once again in danger of falling victim to infighting. Financial Services Committee Chairman Rep. B. Frank (D-Mass.) has requested the formation of a multi-committee task force to craft a single data-security standards bill, in hopes of avoiding the jurisdictional struggle between the Financial Services Committee (FSC) and the Energy and Commerce Committee (ECC) that befell the 109th Congress's attempt to lay down data-security standards. "I want us to start cooperating together, because I do think it is important to get a data-privacy bill, and I think it's one we can do on a bipartisan basis if we deal with the jurisdictional issue," said Frank. However, ECC Chairman Rep. J. Dingell (D.-Mich) has already stated his plans to take back jurisdiction over insurance, securities, and accounting issues that the House transferred to the FSC in 2001. US Public Interest Research Group consumer program director E. Mierzwinski believes that states, which have the ability to improve on the laws of other states, are better suited to set such data-security standards. He feels that business lobbyists are setting their sights on the federal level in hopes of implementing the lowest possible standard for the security of personal financial data. Many congressmen think that the multi-committee group that Frank envisions, the FSC, ECC, and Ways and Means committee, would work well together, with Dingell as the only question mark, but given the wide-ranging concerns of those involved, the legislation they draft may include a variety of privacy and data-security measures. Many are optimistic that the time is right for progress to be made on the privacy front, although there is some disagreement over whether or not privacy and data security are a single issue or if they should be addressed separately. Frank is also considering offering incentives to companies that encrypt their information so a breach would not be disastrous.

The Legal Tangles of Data Collection
Washington Post (01/16/07) P. A9; E. Nakashima

Data collection efforts are being aided by both loopholes and progressing technology, as federal laws struggle to keep up. The Bush administration's assertion that it could tap phone calls without a warrant has gained much attention and opposition, but little has been done to curb such practices, including those concerning email surveillance. The 1978 Foreign Intelligence Surveillance Act and Title III of the 1968 Omnibus Crime Control & Safe Streets Act stated that a warrant is need to tap a phone call; this law was later extended to prohibit interception of electronic communication without a warrant. However, in the 1980s and 1990s when this addendum was made, emails would stay on a user's computer only. Today, email stored on a third party's server can be obtained by the government simply by serving a subpoena, which does not require notification of the user, sometimes even prohibiting notifycation for a certain time. In fact, any information held by a third party is subject to these same rules. Since Sept. 11, 2001, the government has extended its ability to obtain private financial, phone-call, and Internet transaction data, using national security letters that do not require judicial approval; 30,000 such letters were issued by the FBI in 2005. While information can help law enforcement, mistakes have been made and people wrongly accused. Privacy experts say that as more and more personal information is being stored on the Internet and on database over which the individual has little to no control, the law is becoming less capable of protecting citizens.

A DVD Copy Protection Is Overcome by Hackers
New York Times (01/17/07) P. C4; B. Stone

A worldwide group of loosely affiliated hackers has overcome the Advanced Access Control System (AACS) antipiracy software meant to protect HD DVDs and distribute various films online. Less than a month ago, a hacker called Muslix64 released software that allows users to copy HD DVDs onto their computers, but left out the necessary title keys that are generated by AACS software for each movie. Now hackers appear to have found these security keys in DVD-playing programs on their own computers. M. Ayers, chairman of the business group of the trade organization that administers AACS, says that while the intrusion is a serious matter, the hackers have only cracked the DVD-playing software, not the DVD antipiracy system itself. AACS was designed so that players, such as those that have been attacked, could be shut down remotely, by having their licenses revoked. Consultant B. Rosenblatt says this latest intrusion is not as serious as the defeat of the encryption system for standard DVDs in 1999, since HD DVD is intended to "fail more gracefully and not be as brittle as the DVD scheme." However, other experts say the intrusion is more serious. B. Schneier, chief technology officer of security company BT Counterpane, says that while title codes could be changed on new disks, old ones would still be available for some time, and there is little doubt that hackers will increase their efforts to crack new disks. He says, "Data is inherently copyable, just as water is inherently wet. All the technology companies are doing is putting in tricks to make it harder to copy. But all they are is tricks."

Officials Warm to Paper Trail to Verify Votes in Maryland
Washington Post (01/17/07) P. B1; L. Rein

A bill has been submitted in the Maryland General Assembly that would require paper records to back up every vote cast in the state, meaning the state may join a nationwide movement to make touchscreen voting a more trustworthy and secure process. If the bill passes, Maryland would have to retrofit its voting machines with printers, or make a complete switch to optical scan machines. Over $100 million was spent on the state's current voting equipment, which was purchased right after the 2000 election. Maryland's touchscreen voting e-

quipment is relatively early technology and retrofitting it will be difficult and costly. Twenty-seven states have already legislated changes in e-voting to increase reliability, and some states have even gotten rid of touchscreen machines completely. Maryland is one of only five states that use electronic voting systems without providing voters any way to verify their vote. Neighboring Virginia and D.C. use touchscreen machines in some districts or let voters choose between paper and electronic systems. Paper trail advocates expect congressional or state action to require a paper trail for all voters by the 2008 presidential election. Last month, the US Election Assistance Commission recommended that all voting districts either switch to optical scan machines or equip touchscreen machines with printers, since the latter voting machines cannot be secured otherwise.

Malware Creators Turn Code Protection Technique to Their Advantage
ITBusiness.ca (01/09/07), P. Khanna

The programming method known as dynamic code obfuscation, originally developed to protect code against intellectual property theft, is becoming a popular way for hackers to keep their malicious code from being identified, according to Finjan's Web Security Trends Report Q4 2006. Code obfuscation, which allows code to always appears different, is a useful way for programmers to prevent others from figuring out what their code actually does, but hackers can use the technique to foil anti-virus programs that rely upon a virus having a static signature. The technique also allows spammers to hide their intentions. Security consultant M. Kirwan suggests that businesses think of security as something that is built from the ground up, rather than simply being slapped on at the end. Finjan also expects Web 2.0 sites such as Wikipedia and MySpace, both of which recently experienced malicious code-related attacks, Microsoft Vista, and Internet Explorer 7 to see an increasing number of hacker attacks.

Digital Fingerprints
Science News (01/13/07) Vol. 171, No. 2, P. 26; J. Rehmeyer

Neither online criminals nor innocents may be safe from new techniques to de-anonymize Internet users by studying their behavioral patterns. Researchers at Italy's University of Torino are building on the typeprint method, in which a person's identity is determined according to keystroke timing, to craft a system that analyzes typing rhythms to keep track of illicit activity around the Internet. There is concern that such a system would allow authorities to identify innocent users by keeping a log of many individuals' typing patterns, while hackers could conceivably employ the typeprint analysis method to deduce passwords and other critical information. University of Arizona researcher H. Chen led a team that pioneered a program for identifying people by their distinctive writing styles--punctuation, use of the passive voice, indentation, paragraph length, proportions of uppercase and lowercase letters, word choice, content, etc.--so that Internet abusers can be pinpointed through message analysis. The consistency of writers in terms such as word length and punctuation is graphically represented in a writeprint. Chen's team reported in last April's Communications of the ACM that after examining 30-40 messages from any known author, the program could identify subsequent messages by that author with 99% accuracy in English, 95% in Arabic, and 93% in Chinese. The Electronic Frontier Foundation's P. Eckersley is worried that whistle blowing and public speech could be stifled by tools such as writeprints. Identifying people on the Internet by their mouse movements is another technique under investigation, and researchers at the Wharton School in Philadelphia and the University of California, Davis, are focusing on fraud prevention and ID authentication via analysis of clickstream data culled from multiple browsing sessions.