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

Δελτίο 25
18 Μάη 2006

Reversing Course on Electronic Voting
Wall Street Journal (05/12/06) P. A4; J. Cummings

Citing the spate of demonstrated vulnerabilities in e-voting machines, some supporters of the 2002 Help America Vote Act have grown concerned that the law intended to improve the voting process could have made things much worse, and have begun filing lawsuits to block the compliance efforts of some state election officials. The law, passed to ensure that the confusion surrounding the 2000 presidential election is not repeated, requires states to upgrade their voting systems to electronic machines, which at the time were considered more reliable than the archaic paper ballots being used in many states. Arizona was sued last week over the e-voting machines that it purchased with federal money authorized by the act, and a suit is likely to be filed against Colorado election officials next week. The Arizona lawsuit charges that the e-voting machines are unreliable, susceptible to fraud, and that electronic ballots are more difficult to recount than paper ones. The Help America Vote Act "has been turned on its head and it's causing more problems than solutions at this point," said L. Finley, co-founder of Voter Action. Diebold argues that its equipment is secure, and that it runs on technology that has been in use for at least a decade. Several states returned to paper ballots after experiencing glitches in electronic machines in the 2004 election. In addition the charge that they are unreliable, critics of touch-screen systems claim that the sophisticated technology gives too much control over the election process to equipment makers. Investigations into glitches in e-voting systems have uncovered both technical flaws and cases of user error. Although, there has not yet been a proven instance of anyone electronically manipulating votes in an actual election, computer scientists say it's possible. A 2005 report from the Commission on Federal Election Reform warned that "Software can be modified maliciously before being installed into individual voting machines. There is no reason to trust insiders in the election industry any more than in other industries."

French Digital Music Copyright Bill Advances
New York Times (05/12/06) P. C3; T. Crampton

French lawmakers have moved closer toward passing a copyright law that could reshape the landscape of digital music. Bowing to pressure from Apple, the Senate amended the bill to modify the provisions that would have required Apple to make all the music sold at its iTunes store playable on devices other than the iPod. The Senate version of the bill also only allows companies to appeal to the courts to force Apple to open its music, while the version in the National Assembly permits such requests from consumers. The material effect of the legislation on companies such as Apple and Sony will only be determined by committee sessions, but the issue reflects the broader debate playing out around the world over patents and copyrights in the age of Internet distribution. "France has adopted an entirely new and unique approach to managing digital music and films that could be a model for other countries to follow," said Ovum's J. Arber. "Everyone will be watching the impact six months down the line to see whether consumers or companies have benefited." The penalties for piracy are reduced to the level of a traffic infraction and software makers must disclose details of their programs to the government in both versions of the bill. Apple, Vivendi, and Time Warner are aggressively lobbying against the bill, claiming it is tantamount to sanctioning piracy, though the French government argues that it will encourage innovation.

As Tech Advances, Privacy Laws Lag
Los Angeles Times (05/12/06) P. A1; J. Menn; J. Granelli

Privacy laws are struggling to keep up with rapid advancements in data-tracking technology, a fact that was underscored by Thursday's revelation that three of the top telephone companies in the country provided customer calling records to the National Security Agency (NSA). The advent of powerful database tracking programs has made American's personal data easier to collect and distribute than ever before. A wide range of parties, including credit card companies, online retailers, curious neighbors, and county law enforcement, now have the capability to collect this personal data. And companies that collect this type of data can suddenly find themselves at the center of a privacy controversy when their customers' privacy expectations collide with the US government's national security needs, which is what happened when AT&T, Verizon, and BellSouth complied with the NSA's request for customer calling records. Online retailers, such as Amazon.com, use powerful software to make recommendations to customers, and credit card companies also tailor their offers to consumers by tracking consumer purchases. "You have to think about how that information could be misused or used too zealously," says M. Flaherty, a law professor at Fordham Law School.

Three States Mandate More Security for Diebold E-Voting Machines
Associated Press (05/11/06), D. Goodin

Diebold is developing a permanent solution for a flaw in its electronic voting machines that some observers believe could be used to conduct unauthorized functions, and even sabotage an election. Researchers with Black Box Voting, a nonpartisan, not-for-profit organization, discovered the feature that could theoretically allow a hacker to load authorized software on Diebold Election Systems e-voting machines, and the Oakland Tribune reported the vulnerability this week. Black Box Voting also plans to release a report on its finding this week. "It's a deliberate feature that was added by Diebold that we all believe is unwise," says Carnegie Mellon University computer science professor Michael Shamos, who has been briefed on the flaw. Diebold maintains that there has been no evidence that any voting on its machines has been compromised, adding that following its existing security procedures will make it difficult for anyone to take advantage of the vulnerability. Although Pennsylvania officials say someone would need to have physical access to the memory card slot while the system booted up in order to exploit the vulnerability, they have ordered local officials to reinstall the authorized software just before testing Diebold machines and certifying them for use. California and Iowa have mandated similar policies for Diebold computerized machines until the company delivers a permanent solution.

AJAX Experts Tackle Security
eWeek (05/11/06), D. Taft

A group of experts met to discuss the major issues concerning AJAX, such as tooling, security, support, and the stance of Microsoft at this week's AJAX Experience conference. Members of the audience were most concerned about security, and panelist A. Russell, co-founder of The Dojo Toolkit, noted that the basic security issues have not changed over the past five years, and that trust is still at the center of computing security, irrespective of the introduction of AJAX. There have been some recent developments that could optimize the browser capabilities and improve the cross-domain problem, said Brent Ashley, consultant and scripting expert who specializes in AJAX. "There are JSON [JavaScript Object Notation] requests that don't exchange cookies during the request. And [Adobe] Flex and ActionScript have a cross-domain file that says, 'These sites are allowed to cross-domain with me.' That gives some control back to the server side. So while there are issues now, here's a new set of constraints." Some panelists expressed frustration at the lack of compatibility between AJAX and Microsoft's Internet Explorer. Russell also noted that the numerous AJAX frameworks that have emerged generally have a high level of interoperability. When asked about mobile AJAX, Sun's G. Murray said that his company is looking into developing an AJAX platform to support portable devices.

Mining Data to Nab Terrorists: Fair?
Christian Science Monitor (05/15/06) P. 1; M. Clayton

The real value of harvesting the phone records of millions of Americans is the possibility that intelligence analysts could use the data to establish patterns and connections between people that flesh out a network of potential terrorists, according to computer experts. "From phone records you can learn who are my friends--and who their friends are -- what services I use, where I shop," says J. Gehrke, a Cornell University computer scientist. "Our social interactions leave a digital trail. [Phone record analysis] is government learning about human behavior from analyzing that trail." Intelligence analysts likely cross-reference phone records with numerous other data, such as Internet and credit card records, in an effort to extract meaningful relationships from the wealth of digital information available today. As it gathers steam, the data-mining program could run afoul of the law, or grow so large that it creates so many false positives that finding real terrorists actually becomes more difficult. V. Krebs, an expert in social networking analysis, claims that it is more effective to conduct analysis around specific persons of interest, rather than the government's method of amassing vast databases of the activities of mostly innocent Americans, where it will be difficult to conduct accurate analysis due to the sheer volume. Krebs maintains that the government is complicating the problem by taking such a broad-brush approach and that it will inevitably waste time and needlessly intrude on innocent Americans because of the myriad scenarios that could produce a false positive. The Electronic Frontier Foundation (EFF) reports that a single AT&T database contains 300 TB of information, 15 times the size of the Library of Congress. Harvard University law professor C. Fried dismisses the allegations raised by the EFF and other civil liberties groups that the program is illegal, noting that phone records only have the narrowest legal protection.

States Beef Up E-Voting Security After Reports on Weaknesses
E-Commerce Times (05/12/06), K. Regan

States that have purchased the Diebold e-voting machines recently reported to contain a serious vulnerability have been taking steps to improve security for the next elections. Black Box Voting issued a report detailing the work of Finnish computer expert H. Hursti that discovered what one expert called the most serious vulnerability found to date in a Diebold machine. "While these flaws are not in the vote-processing system itself, they potentially seriously compromise election security," the report said. "It would be helpful to learn how existing oversight processes have failed to identify this threat." Diebold notes that hacking the machines would require physical access to them, and that the vulnerability was designed to ensure that the machines could be updated with new software to prolong their lives. Many looked to e-voting as an alternative to the outdated paper systems that created so much confusion in the 2000 presidential election, though critics are worried that the increasing reliance on technology puts too much power in the hands of manufacturers and specialists, and that verifying votes is essentially impossible in machines that do not produce a paper record. The nonprofit group Voter Action has helped voters in Arizona file a suit attempting to halt the state from purchasing e-voting machines, claiming that they would disenfranchise certain voters. Critics are concerned with the chain of custody of the machines, noting that a breach could go unnoticed for a long time because they are frequently moved around and placed in storage for extended durations. A knowledgeable programmer could infect the machines with a malicious program in minutes, according to the Black Box report. Diebold and other e-voting supporters note that there has not been a single reported case of altering an actual election, and that manipulating results from traditional machines is as simple as destroying the paper ballots.

China Says One of Its Scientists Faked Computer Chip Research
New York Times (05/14/06) P. 10; D. Barboza

China has reported that Chen Jin, a prominent researcher and a dean of Jiaotong University, fabricated his research behind one of China's first native-developed computer chips and that he stole the technology from a foreign company. Chen has been dismissed from his government and university positions, and the government has permanently banned him from participating in any government-funded projects. A statement from the prestigious Jiaotong University read, "Chen Jin has breached the trust of being a scientist and educator. His behavior is despicable." Chen developed his three digital signal processors with the funding and support of the Shanghai government, Jiaotong University, and China's top scientific and government organizations. China has made its semiconductor industry a top priority in the face of tensions with the rest of the world over intellectual property issues, and heralded Chen's first chip in 2003 as a major scientific achievement. That chip, known as Hanxin, or China chip, is a high-speed processor for electronic devices such as mobile phones that was introduced as a milestone in China's development of a native semiconductor industry that would help break the foreign monopoly on chip design. The faster Hanxin 2 and Hanxin 3 appeared nine months later, though now Jiaotong and the government say the chips do not have the capabilities that Chen had claimed, despite having reported earlier that government appraisers had tested the chips. The government has canceled the Hanxin initiative and recalled its funding. Allegations that Chen fabricated his findings first appeared on the Internet this past winter, posted by someone naming himself as a whistle-blower.

MS Researchers Tackle Automated Malware Classification
eWeek (05/11/06), R. Naraine

At the recent European Institute for Computer Anti-Virus Research conference in Hamburg, Germany, Microsoft researchers announced their plans to develop an automated technique for identifying the thousands of varieties of malware that target Windows computers. Their approach will utilize distance measure and machine learning technologies to improve on the existing methods of classifying different viruses, Trojans, rootkits, and other forms of malware. "In recent years, the number of malware families/variants has exploded dramatically," says Microsoft's T. Lee. "Virus [and] spyware writers continue to create a large number of new families and variants at an increasingly fast rate." The evolutionary habits of malware families make it extremely difficult to automate static file analysis, Lee said. Microsoft believes that automation would provide a faster, more objective method for malware classification that saves more information than current techniques, which rely heavily on human research and memorization. Microsoft is hoping that its new method will address all aspects of classification holistically, including knowledge consumption, representation, and storage, as well as the generation and selection of classifier models. The technique will require the efficient structuring, storage, and analysis of the classifications so that familiar patterns can be identified immediately.

Password Security Is Her Game
California State University, Long Beach (05/06) Vol. 58, No. 5, R. Manly

Password security is not going anywhere, even though it may not be the most secure form of protection, according to Kim-Phuong Vu of the Psychology Department of California State University, Long Beach. Vu, a human factors expert who specializes in proactive password protection, wants to make passwords more secure and memorable. The editor of the handbook "Human Factors in Web Design" last year, Vu says many people have about six passwords, about half never write them down and have to reset their passwords because they have forgotten them, and she adds that it is not difficult to crack the average password. In fact, she has conducted research that shows 60% of passwords can be cracked within a few hours and some can be determined in less time. People tend to choose something that is easy to remember for their passwords, which makes them easy to crack. A password that is easy to figure out puts bank accounts, grades, Web sites, and more at risk, but people have generally embraced password security, which is affordable. Voice recognition is still not ready, and high-fidelity systems are expensive, as are fingerprint and retina scans, which the typical computer user also finds unsettling. Vu says a combination of higher or lower case letters, numbers, and special characters would make for proactive password protection, and suggests that users would have to spend more time committing passwords to memory.

Young Cyber-Sleuths
Government Technology (05/06) Vol. 18, No. 5, P. 30; J. McKay

The CyberScience Laboratory (CSL) of the National Institute of Justice's Office of Science and Technology places students in cyber-crime labs through the Embedded Intern Program. It is part of CSL's effort to offer computer forensics training and supply local and state law enforcement with personnel to investigate electronic crimes and provide technical support. "We're looking for somebody who can bridge the gap between the physical, investigative, law enforcement world and the computer cyber-world," explains Embedded Intern Program director R. DeCarlo. He adds that demand for cyber-crime investigators will swell exponentially as the Internet and wireless devices continue to proliferate. "There aren't enough computer forensics programs available to grow people in the profession," notes National White Collar Crime Center (NW3C) computer crimes section manager R. Hopper, who points to an international need for more trained cybersecurity workers. Finding the right person for an internship involves a penetrating examination of candidates' backgrounds, including their extracurricular activities and cover letters. DeCarlo says the CSL and NW3C programs take care to ensure that interns work on projects of significance, and that their contributions play a vital role in the agencies where they are embedded. Following the completion of an internship, CSL students are asked to furnish a report that the laboratory features on its Web site and at seminars.