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

Δελτίο 28
7 Ιουνίου 2006

Debating the Bugs of High-Tech Voting
Washington Post (05/´30/06) P. A15; Z. Goldfarb

As midterm elections near, the debate centering on the security of e-voting systems is heating up as voting machine vendors and voting rights activists clash over the severity of a recently discovered vulnerability. The vulnerability, discovered in a Diebold machine several weeks ago in Utah, would enable anyone with a rudimentary knowledge of computer programming to manipulate the code and alter votes in just a few minutes time, security researchers claim. California and Pennsylvania issued a warning to all counties in those states that use the Diebold machines, though the degree of the threat remains a point of sharp disagreement. David Jefferson, a computer scientist at Lawrence Livermore National Laboratory, was shocked when he found out about the threat exposed in Utah, and echoed the "frequently expressed opinion that this is the worst vulnerability we have ever seen." Diebold counters that the vulnerability was a product of design, that it is there to enable the machines to easily receive software upgrades, and that a person could only tamper with election results if given unrestricted access to the machines. E-voting systems came into widespread use after the Help America Vote Act (HAVA) of 2002, which was passed in the wake of the disastrous 2000 presidential election, but electronic machines do not improve the reliability of voting process without a manual paper trail, voting rights advocates argue. While it has never been proven that ballots have been manipulated in an actual election, numerous votes have been delayed by flaws in the technology. The federal Election Assistance Commission, created to assist in HAVA implementation at the state level, claims that it is in the process of improving the election-system certification process, though voting-rights groups in several states have been pursuing legal action to halt the purchase of new electronic systems.

Incidents Prompt New Scrutiny of Airplane Software Glitches
Wall Street Journal (05/30/06) P. A1; D. Michaels; A. Pasztor

As commercial airplanes grow more dependent on increasingly complex computer code, software glitches are emerging as a primary safety concern. The systems in the latest jetliner contain more than 5 million lines of computer code, compared to fewer than 1 million in older models, making it increasingly difficult to locate the flaw when something goes wrong. While the software used in planes is tested far more rigorously than everyday office applications, the errors that inevitably arise can have much more serious consequences, and officials have begun reviewing flight data from earlier accidents to determine what role, if any, faulty software played. "It's our next big area of work," said P. Gillian of the FAA, adding that only recently officials and experts "came to the realization that we haven't looked at this area" closely enough. While no airplane crash has yet been attributed to malfunctioning software, several recent incidents where software glitches have disrupted flights have called attention to the problem. "A total loss of flight control could be worse than a fire on board," said R. McCall, a retired pilot for Delta Air Lines. McCall says that automation programs can make it difficult for pilots to revert to manual controls to overcome a problem. Experts agree, however, that air travel has become much safer since the introduction of automated systems. Today's autopilot systems handle much more of the plane's functions than when they were

first designed, including adjusting the cabin's air pressure, optimizing fuel efficiency, and warning of the threat of collision or mechanical breakdown. Forthcoming models, such as Boeing's 787 Dreamliner, will bring new levels of automation, replacing autonomous hardware and software with redundant central computers. A group of US airlines, pilots' unions, jet manufacturers, and software vendors recently launched a data-gathering initiative to analyze previous computer-related accidents.

Codes on Sites 'Captcha' Anger of Web Users
Wall Street Journal (05/31/06) P. B1; D. Kesmodel

Web sites such as Yahoo.com protect themselves from mischief-making programs by having users who wish to gain access solve puzzles known as "captchas," which often take the form of a visually distorted code that must be correctly typed. Keeping pace with new spamming techniques and strategies has prompted some Web sites to make these codes trickier to solve, irritating more and more Web users. "We know there's no perfect panacea, but we think this is a great tool to prevent malicious activity," says Google engineering director D. Jeske. However, the World Wide Web Consortium published a paper in November 2005 warning that captchas "fail to properly recognize users with disabilities as human" and can be thwarted by clever programmers, as part of its argument for programmers to develop alternative captchas. The group noted, for example, that spam companies sometimes use people rather than automated programs or "bots" to decipher the captchas. Director of the consortium's Web Accessibility Initiative J. Brewer says visual captchas are especially difficult for disabled people because they "don't tell humans and computers apart; instead, they tell able-bodied humans and computers, along with disabled humans, apart." Alternatives some Web sites are exploring or deploying include audio captchas or quizzes that involve simple problem-solving. In development by Lehigh University computer science professor H. Baird are "scatter-type" captchas that fragment each letter in the code, while some sites are simplifying their captchas so humans can solve them easier.

Why the Democratic Ethic of the World Wide Web May be About to End
New York Times (05/28/06) P. 9; A. Cohen

The effort by Internet service providers to impose a new system of fees on the Web poses a threat to Web creator Sir T. Berners-Lee's vision of a platform on which everyone in the world could communicate on an equal basis, writes A. Cohen. The new system of fees could create a tiered Internet that would enable service providers to shut out Web sites whose politics they do not agree with. Even if ISPs did not discriminate on the basis of content, access fees would automatically marginalize smaller, poorer sites. For example, Internet users can now watch video from content providers such as BBC World as well as video blogs and Web sites such as YouTube.com, where people can upload videos of their own creation. However, under tiered pricing, Internet users may be able to get videos only from major corporate channels. Berners-Lee, who has begun speaking out in favor of net neutrality, predicts that the fees could also hamper future innovations, such as a Web site that will allow Internet users to take videos of an event with their cell phones and piece them together to create a three-dimensional image of what happened. He also argues that service providers may be hurting themselves by pushing for tiered pricing, because customers who are used to the Web as it is now may not pay for access to a Web that is restricted to wealthy corporate content providers.

Internet Firms Told to Keep Records on Customers Longer
Washington Post (06/02/06) P. D5; M. Sherman

Internet companies have been instructed by leading law enforcement officials to hold onto customer records for a longer period of time in order to help in investigations of terrorism and child pornography, and a meeting between industry representatives and Justice Department officials to discuss the issue is scheduled for today. Privacy concerns were raised by ISP executives a week earlier at a conference with FBI director R. Mueller and Attorney General A. Gonzales, where the issue of longer record retention was first brought up, according to Assistant Attorney General R. Brand on Thursday. Gonzales has said that some child pornography investigations have been hampered because Internet firms do not keep records long enough. Brand said Gonzales has not yet decided how to move forward and that the Justice Department would give privacy consideration. She insisted that whatever proposal is presented would not mandate the preservation of customers' communications content. The information would be held by the companies, and could be acquired by the government through legal channels. No sweeping requirements exist for preservation of data, though federal authorities can request the maintenance of records for as long as half a year if there is suspicion of criminal activity. Google made an official statement that "Any proposals related to data require careful review and must balance the legitimate interests of individual users, law enforcement agencies and Internet companies."

Data Mining: The New Weapon in the War on Terrorism?
Federal Computer Week (05/29/06) Vol. 20, No. 17, P. 38; A. Sternstein

The data-mining technology needed to support a massive government initiative to ferret out terrorists through analysis of phone records will be costly and computationally intensive, and could compromise the privacy of ordinary US citizens. While it is uncertain if the government is actually using data-mining techniques to sift through the tens of millions of records it has collected from Verizon, BellSouth, and AT&T, it would need supercomputers comparable to IBM's Blue Gene to derive meaningful information from a dataset so large, says N. Hoskin of Planning Systems. Hoskin estimates that such a system would cost between $20 million and $50 million. To effectively mine the data, the system would use clustering algorithms to focus on relationships between similar data, link analysis to find connections between disparate data, and rule mining to find patterns within the data. Privacy advocates warn that giving the government unfettered access to citizens' phone records, even in the name of fighting terrorism, could lead to a host of civil rights violations without ever producing a lead. Critics have compared the possible data-mining initiative to the aborted Total Information Awareness program envisioned by the Defense Department to preemptively combat terrorist attacks by analyzing patterns within a huge repository of electronic data. Data-mining experts say that even if the phone companies are not turning over customers' personal identifying information such as names and street addresses, the government could easily retrieve that information from other databases and services. While data mining does not go as far as wiretapping, privacy advocates warn that the threat is very real. "Listening to the content of calls is more intrusive, but nobody should underestimate the privacy invasion that's involved in tracing who's talking to whom," said the ACLU's J. Stanley, adding that mining records of phone calls for terrorists is inefficient and tantamount to labeling the US population as suspects.

Code Warriors Battle On
Washington Technology (05/29/06) Vol. 21, No. 10, P. 20; D. Beizer

In an effort to update the methods of encryption used by the intelligence community, the NSA and the Defense Department have implemented an ongoing program called the Cryptographic Modernization Initiative. "In the encryption world, probably on a timeframe of every 7-10 years, there's a need for new encryption algorithms," says SafeNet Chairman A. Caputo. "Because every year, the enemy or hackers' tools are getting better, periodically you have to increase the strength of the encryption algorithms. That's what the Cryptographic Modernization [Initiative] does." A major change in the encryption world came when the National Institute of Standards and Technology adopted the Advanced Encryption Standard (AES) in 1991, according to A. Sherman, associate professor of computer science at the University of Maryland. The old system was designed for 56-bit technology, while the current AES is fixed at 128 bits, with key sizes of 128, 192, or 256 bits. SafeNet has received approval from the NSA to develop a classified version of its 10-Gigabit SafeEnterprise Sonet Encryptor for use in federal intelligence agencies and defense and civilian groups. SafeNet's system consists of small, special-purpose computers that encrypt and decrypt traffic at the endpoints of communication nodes. Cryptography experts claim that while software-based encryption is sufficient for most IP traffic, only hardware encryption protects both the algorithm and the encryption key. "Our devices in the field today have encryption algorithms much stronger than commercial encryption algorithms, but you still need to periodically strengthen algorithms to make sure the communications links continue to have good security," Caputo said. In addition to intelligence, government agencies use encryption to protect information such as health and tax records, and Sherman notes the potential applications in securing e-voting systems.

Several Lawsuits Target E-Voting
USA Today (06/05/06) P. 1A; P. O'Driscoll

With the primary election season on the horizon, voting rights groups have filed lawsuits in at least six states to block the purchase or use of computerized e-voting systems. The most recent challenge came in Colorado, where the non-partisan advocacy group Voter Action filed suit last week against the state and nine counties, following similar court actions initiated by the group in California, Arizona, and New Mexico. Other groups have filed lawsuits in Florida, Ohio, and Pennsylvania. Voting rights advocates say the software in e-voting machines is prone to tampering and ballot manipulation, and that election results are unverifiable in the absence of a recountable paper trail. Under pressure from a lawsuit, several counties in California have already dropped their touch-screen voting machines in favor of systems with printed ballots read by optical scanners. Six of eight states holding primaries on Tuesday will use touch-screen systems, which are in use in approximately one-third of counties throughout the US. While there has never been a confirmed incident of manipulating an actual election, a Finnish security expert found significant flaws in a Diebold machine last month. Diebold says the vulnerability is strictly theoretical, and that it will be fixed later this year. E-voting defenders claim that problems typically occur when poll workers are inadequately trained or when the systems are hastily set up. "Certainly none of the allegations of security breaches on the equipment have ever been demonstrated to be true," said R. Doug Lewis of the Election Center. Many states began investing in e-voting systems after Congress authorized more than $300 million to replace outdated voting machines under the Help America Vote Act.

Government, Internet Firms in Talks Over Browsing Data
Washington Post (06/03/06) P. D3; F. Ahrens

The US Justice Department and FBI are holding discussions with leading companies in the Internet field to convince companies to retain data on Web surfing for possible use in child pornography and terrorism cases. Google, Yahoo!, AOL, Microsoft, and others are involved in the negotiations, and Microsoft has stated that the issue of consumer Internet privacy and retaining data is best seen as a balance of privacy and law enforcement concerns. The Justice Department and FBI may seek legislation from Congress requiring data retention. They hope to base their request on a potential industry consensus solution outlined in these ongoing negotiations. However, in the first meeting between the Justice Department and the companies, government officials were stern in their demands. The second meeting featured more of a dialogue. Internet companies are wary of changing the current process so drastically that it degrades consumer privacy on the Internet. Currently ISPs and Internet companies refer possible illegal activity online, such as viewing child pornography, to law enforcement officials. Officials then must return with a warrant or subpoena to obtain Web surfing records.

Security Researchers to Produce New Tools
Concordia Journal (06/01/06) Vol. 1, No. 15, B. Black

Cybersecurity has emerged as the most important challenge for computing researchers ever, according to M. Debbabi, a Concordia Research Chair who is leading a security research project with almost $1 million in joint funding from Bell Canada and the Canadian Department of National Defense. "The tremendous success of Internet-related technologies, such as Web services, voice-over IP, mobile telephony, and so on, coupled with advances in hardware and software engineering are giving rise to challenging and very interesting research problems," he said. The project's first initiative will focus on securing free and open-source software. The second phase will formulate tools and techniques for conducting forensically sound investigations of cybercrimes, collecting evidence and verifying and sequencing information to support the work of law enforcement.

Online Throngs Impose a Stern Morality in China
New York Times (06/03/06) P. A1; H. French

The Internet is increasingly being used by Chinese users to investigate others and mete out punishment for morality offenses both real and imagined. For example, Chinese Internet users have used the Web to scrutinize husbands suspected of cheating on their wives, investigate fraud on Internet auction sites, examine the secret lives of celebrities, and look into unsolved crimes. In one recent incident, a man used an Internet bulletin board to accuse a college student of having an affair with his wife. Within days, hundreds of thousands of anonymous Internet users formed teams that hunted down the student, forced him to leave his university, and caused his family to barricade themselves inside their home. The phenomenon, known as Internet hunting in China, is setting off alarm bells in the country. Many are comparing it to the Cultural Revolution 40 years ago, when mobs of students taunted and beat their professors. Mass denunciations and show trials were also common during this period. In order to deal with the problem, the government is considering registering all Internet users. However, free speech advocates say there is no reason for the Chinese government to place such restrictions on the Internet. "The Internet should be free, and I have always opposed the idea of registering users, because this is perhaps the only channel we have for free discussion," said Z. Dake, a sociologist and cultural critic at Tongji University in Shanghai. "On the other hand, the Internet is being distorted. This creates a very difficult dilemma for us."

The Code That Keeps Your Fingerprints Secure
New Scientist (06/03/06), C. Biever

Researchers at the Mitsubishi Electric Research Laboratories (MERL) have developed a technique that secures biometric information by creating a second code that can not be used to recreate the biometric. The algorithm comes at a time when the government and companies are storing the biometric information of millions of people, and there are concerns that it would not be difficult for thieves to gain access to a biometric and then use it to steal a digital identity. Conventional biometric systems store the raw details of fingerprints, iris scans, and facial images. However, the algorithm from E. Martinian and his colleagues at MERL does not store the raw materials, but manipulates the code to produce a shorter code called a syndrome. The algorithm is designed to manipulate the ones and zeros of a biometric code and as a result, gaining access to a syndrome will not do a hacker any good because he would have no idea how to find its match in order to "correct the error" and reconstruct the original biometric. "The only person who should have your fingerprint is you, on the end of your finger," says MERL director J. Marks. Martinian says the algorithm is safer than the warped biometric system being developed by IMB researchers, which he maintains would not be able to prevent a thief from using a warped biometric to decrypt the data.

The Enemy Within: Terror by Computer
New Zealand Herald (06/01/06), J.L. Shreeve

If terrorists turn their attention away from the physical to the digital world, there may be even greater damage than the Sept. 11 attacks, say cyber-security experts. Computer network attacks are dangerous enough to kill people and destroy companies, according to S. Borg at the US Cyber Consequences Unit. "Up to now, executives and network professionals have worried about what adolescents and petty criminals have been doing," says Borg. "In most cases, these kinds of cyber attacks aren't very destructive. The reason is that businesses generally have enough inventory and extra capacity to make up for short-term interruptions." In the past, hackers focused on credit cards or personal information found on the Web, but now they are starting to focus on databases. Borg gives examples of possible scenarios such as the tampering of a pharmaceutical company's database or changing specifications at a car factory, which may cause a car to catch on fire. Those kinds of attacks could crash the economy with just the click of a mouse, according to Borg. Officials say their biggest fear is over electronic attacks that focus on the networks that make up the critical national infrastructure. "People claim no one will ever die in a cyber-attack, but they're wrong," says R. Clarke, a former cyber-security expert in the Bush Administration. "This is a serious threat."