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

Δελτίο 85
31 Ιουλίου 2007

Senators to Abandon '08 E-Voting Paper Trail Mandate
CNet (07/25/07), A. Broache

Democratic senators made another push to ban electronic voting machines that do not provide a paper trail, but decided not to try to force states to do so by next year's presidential election. Sen. D. Feinstein (D-Calif.), the chief sponsor of the Ballot Integrity Act, which proposes such a ban, says she fears requiring all states to use voter-verified paper records in time for the next election "could be an invitation to chaos," as some primaries are only six months away. "Pushing the date back to the 2010 elections will give us more time to reach a bipartisan consensus ... to enact a new law that provides for increased accuracy and accountability at the polls without raising the specter of creating major new errors," Feinstein says. Election watchdog groups and computer scientists have long argued that paper ballots are one of the best ways for voters to be able to verify their vote was correctly recorded, particularly since touch-screen machines have proven to be vulnerable to security flaws and glitches. However, election officials and some voting machine reviewers have argued that paperless machines are not as faulty as some critics claim and that replacing them would be time consuming and expensive. Some of the provisions in Feinstein's proposal would immediately halt the purchase of direct-recording electronic voting systems that do not provide paper records, allocate $600 million for states and localities to replace or adapt paperless machines as necessary, and allow voting machine software to be inspected by state and federal authorities.

NASA: Computer Bound for Space Station Sabotaged
USA Today (07/26/07), T. Halvorson

An employee at a NASA subcontractor purposely damaged a computer that was to be placed aboard the space shuttle Endeavour, which is slated for launch on Aug. 7. Among other things, the subcontractor produces sensors that are placed within space shuttle wings. The damaged computer was scheduled to be delivered to the international space station, where it would have been used as part of an engineering evaluation of space station gauges. NASA's B. Gerstenmaier declined to comment on the motivation behind the sabotage, which is under investigation by NASA's Inspector General. The damaged computer will be repaired and placed aboard the shuttle in time for the launch, NASA officials said. The subcontractor notified NASA about the sabotage earlier this month. The damage to the computer was obvious and easy to spot, consisting of wiring that had been cut; a qualification unit at the subcontractor factory also had wiring that had been slashed.

Future of HTTP at Center of Debate
Network World (07/25/07), C. Marsan

A gathering of leading Internet engineers at an IETF conference in Chicago this week focused on whether the Hypertext Transfer Protocol (HTTP) should be completely reworked to fix well-known security flaws or merely tweaked to address the most pressing errors. Internet experts are aligning themselves on both sides of the debate. Web inventor T. Berners-Lee, the World Wide Web Consortium, and engineers from Microsoft, Adobe, and Hewlett-Pac-

kard all believe that minimal corrections is the right approach at this time and provided some recommendations for adjusting HTTP in a document published by the IETF. "The current plan is to incorporate known errata, and to update the specification text according to the current IETF publication guidelines," the document says. Those who believe a complete overhaul is necessary say requiring authorization mechanisms for HTTP would make the system more secure and help eliminate the widespread problems of spoofing and phishing, even if it sacrifices anonymity. "We need to clean this mess up and that means facing the reality of HTTP security," says J. Klensin, an email pioneer, former executive for AT&T and MCI Worldcom, and former chair of the Internet Architecture Board, an IETF oversight group. Klensin argues that fixing known errors in HTTP and its authentication weakness needs to be accomplished in parallel with each other. Participants in the IETF debate supported establishhing a working group to fix HTTP's shortcomings and to create a document that outlines known security holes. The IETF has twice tried to establish a working group to fix HTTP problems and failed. "It's and interesting time for HTTP," says Yahoo engineer M. Nottingham, who led the HTTP debate. "There have been other attempts to revise RFC 2616 ... I do think this is a unique opportunity to get it done."

Congress: P2P Networks Harm National Security
CNet (07/24/07), A. Broache; D. McCullagh

At a congressional hearing on Tuesday, politicians said peer-to-peer networks constitute a threat to national security by their ability to facilitate the unintentional sharing of sensitive or classified documents by federal workers through their computers. Government Reform Committee Chairman Rep. H. Waxman (D-Calif.) reported that he is considering new legislation out of concern that such documents could be accessed by foreign governments, organized crime, or terrorists. Attending the hearing was Lime Wire Chairman and Lime Group CEO M. Gorton, who came under fire for offering his LimeWire P2P software, which has provided "skeleton keys" that allow people to access national security information, claimed one representative. Evidence that P2P networks can expose sensitive data reflects "the importance of strengthening the laws and rules protecting personal information held by federal agencies" and other organizations, declared ranking committee member Rep. T. Davis (R-Va.). M. Koelbel Engle with the Federal Trade Commission's Bureau of Consumer Protection noted that the threat of sensitive information disclosure has less to do with P2P technology itself than how people employ the technology. Waxman said he was not pursuing a prohibition on P2P networks, which has been proposed in the past, but instead desired striking a balance that shields important federal, personal, and corporate information and copyright statutes.

Government Reports Cybercrime Poses National Risk
InformationWeek (07/24/07), S. Gaudin

The public and private sectors are threatened by ever-increasing domestic and foreign cyberattacks on operational security and law enforcement, concludes a new Government Accountability Office report. The GAO reported that more stringent security must be employed by IT managers, while federal and commercial sectors are faced with ongoing difficulties in detecting Web-based crime. Rep. J. Langevin (D-R.I.) of the subcommittee on Emerging Threats, Cybersecurity, and Science and Technology said that compromised federal Web sites, classified email susceptible to unclassified networks, and infiltration of Dept. of Homeland Security networks are among the government's security challenges. The DHS and its CIO Scott Charbo were faced with reports during a congressional hearing that the department had

experienced 844 "cybersecurity incidents" within two years. Rep. B. Thompson (D-Miss.) wrote that the DHS is at the forefront of cybersecurity for the nation yet department investigations have demonstrated that "'information security' has become an oxymoron." Langevin said China has been "coordinating attacks against the Department of Defense for years," and that potential malware could infiltrate first-strike attacks on US computer systems. "I encourage all businesses--small and large--to take a very close look at their cybersecurity practices," Langevin said. "Though 100% security may be unattainable, there are many policies and procedures that businesses can implement to better safeguard their data."

What Can Be Done About Software Security?
SD Times (07/01/07)No. 177, P. 37; D. Worthington

Problems with project management and organizational commitment and training were traced by experts to be the most frequent root causes behind the increasing incidence of software code vulnerabilities, and tight schedules and a lack of management-defined standards were among the factors cited as contributing to software security deficiencies. SPI Dynamics co-founder Caleb Sima commented that security must be a process that encompasses the entire organization and that is embedded within the existing development life cycle, and he and other experts concurred that companies with a serious security investment must make a bigger commitment to quality assurance tooling, realize the effective use of such tools, and secure developers capable of using those tools to write vulnerability-free code. Intelligent Decisions' director of security business units Roy Stephan advised the establishment of best practices emphasizing boundaries, where applications communicate via protocols or between libraries, and also supported peer code reviews. Consultant R. Black explained that organizations currently lack an incentive to invest more in security because they can pass the cost of security failures on to users and consumers, and he suggested that government intervention might divert the cost back to companies, spurring a corporate interest in patching security flaws. Oracle program director J. Heimann aimed criticism at entry-level developers' prowess, complaining about a dearth of secure coding classes offered by university computer science and training programs. "They do good things, but this is basic knowledge that software engineers should have," he said. Heimann attested that most academics have little secure code development skill, have no desire to teach such a subject, and do not wish to be criticized for their lack of knowledge; he indicated that accreditation standards should impel program revisions that would enable qualified faculty to teach secure programming.

Accessibility Isn't Only Hurdle in Voting System Overhaul
New York Times (07/21/07) P. A11; C. Drew

Efforts in Congress to create legislation that would establish an easy-to-use and traceable voting system stalled again as tension arose over conflicting objectives for the system. The ultimate goal is to create a system that is affordable, uses durable paper ballots or leaves a paper trail, and can be used by disabled voters without help from poll workers. However, conflict between the desire to make every voting machine accountable and other needs, including the desires of the disabled and state budgets, caused the movement to stall. Voting analysts say the tensions made it easy for Democrat leaders to postpone the most drastic changes until 2012, four years after originally planned, a decision that was disclosed July 19. Congressional leaders are hesitant to tell states to throw away hundreds of millions of dollars of relatively new voting machines until it is clear that better technology is available. A proposed compromise also drew heavy criticism. Although 28 states now require that voting machines provide a paper record of each vote cast, many jurisdictions do not. Voting experts said a

stopgap proposal to add spool-like printers to touch-screen machines for 2008 and 2010 would not be possible in some of the states that currently do not print out ballots, forcing them to make larger changes by next year. Meanwhile, efforts to guarantee equal access to disabled votes could cause a delay in replacing touch-screen machines with optical-scan systems, which use sturdier paper ballots. Due to touch-screen reliability fears, about half of the U.S.'s counties use optical-scan machines, and most analysts expect that any federal legislation would promote the use of scanners.

IPhone Flaw Lets Hackers Take Over, Security Firm Says
New York Times (07/23/07) P. C4; J. Schwartz

Researchers at Independent Security Evaluators have discovered a vulnerability in Apple's iPhone that hackers can exploit to take control of the device. Independent Security's A. Miller, a former National Security agency employee with a doctorate in computer science, recently demonstrated to a reporter how a hacker can take advantage of the vulnerability to gain access to the personal information stored on an iPhone. In his demonstration, Dr. Miller used his iPhone's Web browser--a version of Apple's Safari Web browser--to visit a Web page that he designed. Once he had logged onto the site, the Web page injected a bit of code into the iPhone that made the device transmit a set of files to the attacking computer that included recent text messages, telephone contacts, and email addresses. Dr. Miller noted that hackers could also use the vulnerability to program the phone to make calls or turn it into a portable bugging device. S. Bellovin, a professor of computer science at Columbia University, said the hack appears to be genuine. He added that such vulnerabilities are inevitable, given the fact that cell phones are becoming more and more like computers. "We've been hearing for a few years now that viruses and worms were going to be a problem on cell phones as they became a little more powerful, and we're there," he said. Bellovin noted that the iPhone is a full-fledged computer, "and sure enough, it's got computer grade problems."

MIT Encryption Pioneer Rivest Wins Marconi Prize
MIT News (07/17/07)

MIT professor Ronald Rivest has been named the 2007 Marconi Fellow and prizewinner for his innovative work in cryptography and computer and network security. Rivest is the Andrew and Erna Viterbi Professor in MIT's Department of Electrical Engineering and Computer Science, and is known for having helped develop one of the world's most widely used Internet security systems, public key cryptography, which allows users to create and share secure information on an insecure connection. Public key cryptography uses two keys, one known to everyone and one known only to the recipient. The public and private keys are paired so that only the public key can be used to encrypt messages and only the corresponding private key can decrypt them. Even if someone knew the public key, it would essentially be impossible to determine the private key. The RSA encryption algorithm that Rivest created (with A. Shamir and L. Adleman) relies on the challenge of factoring large prime numbers, normally over 250 digits long. The receiving computer secretly selects two prime numbers and multiplies them to create a "public key," which can be posted online. The sending computer can take that public key, enter it into the RSA encryption algorithm, and encrypt the message. The system works because only the recipient knows the prime factors that were used to make the public key, and that is what is needed to decrypt the message. Marconi Society Chairman R. Lucky said, "Public key cryptography has flattened the globe by enabling secure communication via email, Web browsers, secure shells, virtual private networks, mobile phones and

other applications requiring the secure exchange of information." Rivest, Shamir, and Adleman are recipients of the 2002 ACM Alan Turing Award.

E-Voting Systems 'Hacked' for Flaws
San Jose Mercury News (CA) (07/23/07), S. Harmon

As part of a "top-to-bottom" review ordered by California's Secretary of State D. Bowen, several computer scientists recently finished two months of testing to see if the state's touch-screen voting machines should be certified for use in the upcoming elections. The testing included general hacking and attempts to manipulate the voting systems. Bowen is expected to give a report on Aug. 3, six months before the Feb. 5 presidential primaries, but election officials are worried that there may not be enough time if the systems are determined to be vulnerable. The level of testing Bowen's hackers put the machines through is unprecedented and went farther than any other state or federal testing of electronic voting machines, according to Kim Alexander, president of the California Voter Foundation. "Previous testing looked at whether the systems work the way vendors said they're supposed to work," Alexander says. "It didn't include scenarios that would crop up in real elections, such as a software attack or the taking down of a polling place through technical manipulation." County registrars are worried that the decertification of any of the machines could lead to a shortage of machines on election day and some criticized the testing process as unnecessary. "Show me where the systems have actually been hacked and where votes have been changed," says Contra Costa Country registrar and California Association of Clerks and Election Officials president S. Weir. "There's no evidence of it." Weir also says the tests did not account for the defenses that clerks set up to prevent security breaches.