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

**Δελτίο 74**
**16 Μάη 2007**

### Leahy, Others Speak Out Against New ID Standards
**Washington Post (05/09/07) P. D3; E. Nakashima**

Citing concerns about American's privacy, Senate Judiciary Committee Chairman P. Leahy, D-Vt., said that he will push to repeal the 2005 Real ID Act, which is aimed at creating new government standards for driver's licenses and requires states to comply by 2008. States can request more time, but after 2013 anyone with IDs that fail to meet the standards will be barred from boarding planes or entering federal buildings. Leahy has co-sponsored bipartisan legislation to repeal the provision, and a similar Democrat-backed bill is pending in the House. To date, seven states have passed laws or resolutions opposing implementation of Real ID, 14 states have legislation pending, and the DHS has received more than 12,000 public comments in response to the rules. The Real ID legislation was tacked onto a 2005 emergency spending bill by House Republicans, without any debate in the Senate, and was signed by President Bush. The bill's passage interrupted negotiations between state and federal government organizations. Advocates of a repeal want to restart negotiations, but supporters of the Real AD Act say the effort to strengthen state-issued driver's licenses security standard is a key recommendation from the 9/11 Commission. Critics warn that the proposed rules to implement Real ID's national database creates the possibility of privacy invasions and increases the risk of identity fraud.

### USACM Urges Revisions to National Identification Policy
**AScribe Newswire (05/08/07)**

ACM's US Public Policy Committee (USACM) issued a series of recommendations on May 8, citing serious flaws in the nation's Real ID Act. The Real ID Act is intended to establish a national identification system by requiring states to collect, maintain, and share personal information, as well as issue a standard form of identification to all Americans. USACM said the proposed regulations are inadequate to properly protect privacy, ensure security, and maintain accurate personal information. USACM also said the regulations fail to establish clear standards for states to use in the implementation of standard driver's licenses and identification cards. "The policy behind Real ID has been flawed from the moment Congress proposed it. Without sufficient safeguards, it has the potential to enable identity theft on an unprecedented scale. The proposed rules are at best vague in addressing privacy, security and accuracy risks, and at worst, they increase these risks," USACM Chair and Purdue University computer science professor Eugene Spafford said. "States are likely to be financially strapped when they begin to implement Real ID. Simply punting the implementation details to the states is a recipe for disaster. We could see a multitude of standards with minimal resources dedicated to ensuring that privacy, security and accuracy concerns are addressed." USACM said the proposed regulations fail to specify minimum standards or accountability for states to manage state-to-state data exchanges openly and comprehensively.

### Electronic Voting May Be Ready by Fall '08, Official Says
**New York Times (05/08/07), J. Hicks**

New York State Board of Elections co-chairman D. Kellner said New York State may be able to replace its aging voting machines by September 2008, despite predictions to the contrary. Earlier this year, Kellner said most members of the Board of Elections agreed it would be better if the state did not have to make changes during the 2008 presidential election, which is expected to have a high voter turnout. Now, however, Kellner said that although there is little to no chance the new machines would be ready for the state's presidential primary in February 2008, they could be installed by the November 2008 presidential election, and possibly in time for the primary elections for Congress and the State Legislature in September 2008. "If we certify the new machines by December, they should be able to get most of the system in place for the November 2008 election," Kellner said. "And I think the September primary, too." Debate over replacing New York's voting machines has been rocky, and New York is the last state to update its voting machines, despite a federal mandate requiring it to do so. A significant portion of the delay comes from questions about the laboratory testing required for the potential machines being offered by five bidders. At a state Congressional hearing, several voting machine experts testified about a number of problems concerning new electronic voting machines, including conflicts of interest in the testing process and questions about the security and reliability of the machines currently in use. "The testing labs are failing to weed out insecure and unreliable voting systems," said one of the experts, University of California at Berkeley computer science professor D. Wagner. "The federal certification process has approved systems that have lost thousands of votes and systems with serious security vulnerabilities."

### U.S. Critical Infrastructure in Serious Jeopardy
### CSO Online (05/04/07), A. Turner

The US critical infrastructure's heavy reliance on networks has made it extremely vulnerable to exploitation by hackers, but this threat is still not fully comprehended by vendors, asset owners, incident responders, or information security experts, writes A. Turner of Idaho National Labs (INL). History has shown that increasing system complexity carries more dramatic social and economic ramifications in the event those systems become unwieldy or critically vulnerable, and it was the absence of coordinated oversight and planning in the deployment of those systems that led to incidents such as the 1929 stock market crash and the global Internet worm epidemic in 2003. Control system security reviews funded by the Depts. of Energy and Homeland Security and performed by INL have uncovered weaknesses in all the assessed systems that could be exploited by attackers with a low level of expertise, and who do not need to access the systems physically in order to wreak havoc. The INL experts determined that currently implemented systems cannot support the easy deployment of augmented security controls while also sustaining basic system functionality. Turner remarks that the current strategy for guaranteeing system resiliency is highly fragmented, resulting in a situation in which "information security professionals have had to continue to shift resources as the threats and vulnerabilities constantly change from day to day, with very little time to look at the problem and limited resources to coordinate a long-term strategy." Among the factors contributing to the critical infrastructure's vulnerability is asset owners' increasing willingness to link their control systems to the Internet in order to become more efficient and competitive; vendors' continued production of infrastructure system components that lack sufficient safeguards or an overarching security framework; sparse awareness of control system security issues and little public disclosure of serious incidents; and increasingly skilled hackers. Turner concludes that the only real solution for this state of affairs is to "maximize cooperation among asset owners and technology vendors to understand and improve control system security across the entire lifecycle of this necessary and critical technology."

**The Disruptive Power of Networks**
**Forbes (05/07/07), V. Cerf**

Google chief Internet evangelist V. Cerf points out that the Internet has yielded many benefits (users generating information, massive group interaction, widespread and nearly instant access to information, communities formed through social networking) and dangers (invasions of privacy, identity theft, security vulnerabilities). "Overall, though, the disruptive aspects [of networks] will, I believe, have positive effects, giving ample impetus to the creative energy of our global community," Cerf reasons. He anticipates a vast proliferation of Internet-connected devices, including office gadgets and household appliances, while neural interfaces to computer-based systems will also emerge. Computerized and real worlds will be integrated, with interactions that take place in a virtual environment having real-world impact, predicts Cerf. Whole populations could be tracked to spot key health trends or epidemiological threats early via the aggregation of personal health monitoring, while cars and buildings could be equipped for self-awareness and self-guidance. Cerf projects that mobile-knowledge robots will sift through the Internet's data for correspondences and unforeseen patterns, flagging items of interest to users. "As computing power, memory and transmission speeds continue to increase, opportunities to develop new products and services will multiply," he concludes.

**House Panel Approves E-Voting Paper Trails**
**CNet (05/09/07), A. Broache**

The House Administration Committee approved an amended version of the Voter Confidence and Increased Accessibility Act on May 8, with a six-to-three vote along party lines. The bill, chiefly sponsored by Rep. R. Holt (D-N.Y.) and backed by 212 members of Congress, would require all US voting systems to produce or use verifiable paper ballots in time for the next presidential election, as well as require several new security obligations such as a general ban on any wireless technology in the machines and on connecting devices used to record or tabulate ballots to the Internet. All voting precincts nationwide would have to conform to the new requirements in time for the general federal election in November 2008. The bill provides an extra $1 billion, more than triple the original amount proposed, to distribute to states during the 2007 fiscal year to help them update their systems. The Republicans who voted against the bill said they were told that the requirements were unrealistic and impossible to reach by 2008. The bill will also require states to conduct random, hand-counted audits of select percentages of the voter-verified paper ballots cast in a race, except when a candidate is uncontested or receives 80 percent or more of the vote count. "We've never had that in elections, even before voting machines came in," said B. Simons, former ACM president and chairwoman of its e-voting study group. "This is a really enormous change, and just from a security perspective, it makes a big difference."

**Association for Computing Machinery Applauds Committee Vote on E-Voting Reform Legislation, AScribe Newswire (05/09/07)**

The Voter Confidence and Increased Accessibility Act of 2007 addresses much of the concern that the computing industry has for electronic voting, according to B. Simons, a member of ACM's US Public Policy Committee (USACM). She says passage of H.R. 811 by the Committee on House Administration is needed if the e-voting system is to be reformed. The voting process needs to be protected against security risks, software bugs, and equipment failure, says the computing community. Introduced by Rep. R. (D-N.J.), the bill offers specific rules for paper records, manual audits, improving transparency, and testing and certifying e-voting systems. "The approved legislation acknowledges the standards set by USACM to protect the accuracy and impartiality of the electoral process," says Simons, chair of US-ACM's voting subcommittee. The bill now goes before the full House for vote.

**Hackers, Experts to Probe E-Voting**
**Inside Bay Area (CA) (05/10/07), I. Hoffman**

California Secretary of State D. Bowen on Wednesday announced that the state will thoroughly review its electronic voting systems with the help of computer scientists, hackers, and technology policy analysts from the University of California and several other universities and private firms. Experts say it will be the toughest and most thorough review of voting systems in the nation. Three teams will be assembled by two computer security experts from UC Berkeley and UC Davis. One team will look for vulnerabilities in the software of the eight primary voting systems used in the state, another will attempt to attack the voting hardware, and the third will explore the systems' documentation. A fourth team, led by Campbell-based electrical engineer and computer scientist N. Runyon, will analyze the accessibility of every voting machine according to the latest federal standards and test the machines' accessibility for a range of disabled voters. Election officials have complained that they should be more involved in the program, and only one of the eight voting machine companies, Sequoia Voting Systems, has offered their full cooperation. No other vendors have submitted machines for testing yet, and only a few have signed agreements to do so, according to local election officials. Bowen said that she may withdraw approval of any machines that are not provided for testing or that fail the test so badly that their deficiencies are determined to be unfixable. "There has never been as comprehensive a review of voting systems as is contemplated here, and you just could not assemble a better team of people to do it," said Lawrence Livermore National Laboratory computer scientist D. Jefferson, a voting-system expert who is not involved in the review.

**Shredded East German Files Reassembled**
**Associated Press (05/09/07), D. Rising**

Germany has invested $8.53 million in a pilot project to reassemble millions of files that the East German Stasi secret police shredded as the Berlin Wall fell in 1989. About 16,250 sacks containing 45 million pieces of shredded documents were found and confiscated within a year, but efforts to reassemble the documents have resulted in the reconstruction of the contents of only 323 sacks over the past 12 years. The Frauenhofer Institute for Production Systems and Design Technology believes the use of new computer technology will be much more effective, estimating it would take 600-800 years for a team of 30 people to put all the documents back together by hand. Using the Berlin institute's algorithm, German researchers will attempt to reassemble the documents of 400 sacks in two years. A successful pilot could clear the way for a larger initiative of putting together the contents in all of the remaining bags in 4-5 years. The algorithms were used to decipher the lists of Nazi concentration camp victims 15 years ago. The researchers will scan both sides of each individual strip of shredded file, then feed the data into a computer, which will use color recognition, texture analysis, shape and pattern recognition, machine and handwriting analysis, and recognition of forged official stamps to interpret them.

**Google Searches Web's Dark Side**
**BBC News (05/11/07)**

Google researchers are studying billions of Web sites in an effort to identify all possible malicious pages on the Internet. Google researcher N. Provos and his colleagues subjected 4.5 million Web pages to "in-depth analysis" for their paper, "Ghost in the Browser," and found about 450,000 Web pages able to launch "drive-by downloads" and an additional 700,000 potentially compromised Web pages. Drive-by downloads are malicious programs that install automatically when a user enters a "booby-trapped" site, often those with adult video thumbnails or other "interesting" content. Drive-bys frequently install themselves by taking advantage of vulnerable elements in Microsoft's Internet Explorer browser. Virulent code often resides in widgets and banner advertisements, and forums and blog postings containing links are new channels through which criminals can attack. Hackers can hijack entire Web servers, or individual computers; they also can use drive-bys to capture sensitive information. To keep computers safe, Google alerts users with a message if they are about to visit a potentially dangerous Web site. In addition, the company is striving to detect and map all Web-based infection vectors. "Finding all the Web-based infection vectors is a significant challenge and requires almost complete knowledge of the Web as a whole," wrote the Google researchers.

### Java Security Traps Getting Worse
**eWeek (05/09/07), L. Vaas**

In a recent interview with eWeek, Fortify Software founder and chief scientist B. Chess said that Java security traps have only become more of a problem in the year since he gave a presentation titled "12 Java Technology Security Traps and How to Avoid Them" at JavaOne. Chess arrived at this conclusion after Fortify ran the Java Open Review project, which uses FindBugs--a static analysis tool that looks for bugs in Java code--to look over code in a number of open-source projects. After more than a year of running the project, Fortify found that the defect density of open-source code is "astronomical." Java expert William Pugh agreed with Chess' conclusion that Java security traps--particularly XSS (cross-site scripting)--are getting worse. "Tools like Fortify's tool set will look for problems with XSS, but it's not easy to cleanse your code of any XSS [vulnerabilities]," said Pugh, a computer science professor at the University of Maryland. "The statistics we've seen is that this is on its way to becoming the biggest vulnerability" in Java applications, if not all Web attacks. Despite the growing number of vulnerabilities in Java applications, Chess said he has not seen developers working on secure Java coding practices. He noted that a more effective way to address the rising number of vulnerabilities in Java applications could be to talk to framework owners and software makers to see what can be done to make the Web a safer place to program, though that tactic is not likely to be a quick fix, either.

### Escaping the Data Panopticon: Prof Says Computers Must Learn to 'Forget'
**Ars Technica (05/09/07), N. Anderson**

Improvements in technology are turning us into digital pack rats, which is not good for society, suggests V. Mayer-Schonberger, a professor in the JFK School of Government at Harvard. In a faculty research working paper entitled "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing," Mayer-Schonberger says fast processors and affordable storage has enabled our computers and other gadgets to remember everything for us, but a return to an era of "forgetfulness" is necessary. These days, everything from Google searches, family photos, books, credit bureau information, air travel reservations, government databases, and archived email is stored. Mayer-Schonberger says the information can be easily combined to create a composite picture of individuals, and ultimately discourage people from speaking and acting out of fear that the information could be used against them. Mayer-Schonberger's solution is to use legislation and technology to ensure that all computing technology has a default setting to forget data after a certain amount of time. But he adds that users should also have the option to extend the expiration date for as long as they want.

### Cracks in the Air
### Government Computer News (05/07/07) Vol. 26, No. 10, W. Jackson

In a recent lecture at the CIO Council's quarterly IT forum in Washington, Justice Department information technology security specialist M. Kwon gave a sobering assessment of some of the security risks involved in using wireless communications. For example, Wi-Fi technology used in wireless local area networks has a number of vulnerabilities, including rogue access points that can make control difficult, signals that are easy to detect, and encryption standards that are easy to crack. As part of her lecture, Kwon--along with R. Del Gaizo, a computer science student at George Washington University--demonstrated how hackers crack the encryption standards used in Wi-Fi networks. Kwon and Del Gaizo were able to crack the Wired Equivalent Privacy (WEP) encryption standard in just a few minutes after capturing relatively few packets, though they had much more difficulty breaking the Advanced Encryption Standard used in Wi-Fi Protected Access/2 (WPA/2). However, Kwon and Del Gaizo were eventually able to subvert the encryption standard by attacking the passphrase exchange during the connection process. Given these vulnerabilities, Kwon advised users who set up wireless networks to separate the wired and wireless segments with a firewall and avoid anything involving sensitive information on the wireless side of the network. Kwon and Del Gaizo also demonstrated how to hack Bluetooth, a wireless technology that is becoming common for hands-free cell phone communications and for the on-board computers in cars. The two showed how hackers can use a man-in-the-middle attack to intercept a cell phone call. Similar attacks can also be used to steal data stored on a Bluetooth-enabled device, Kwon and Del Gaizo said.