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

Δελτίο 50
1 Δεκέμβρη 2006

E-Voting Measures Sought to Avoid Disputes
San Jose Mercury News (CA) (11/29/06), F. Davies

California Senator D. Feinstein, who will take over the Rules and Administration Committee that oversees how federal elections are run, has made it clear that she will scrutinize the e-voting process. "It's imperative that Congress does everything it can to help ensure that votes cast are recorded accurately," Feinstein said. "Serious questions have arisen about the accuracy and reliability of new electronic voting machines." Even before the previous election, in which Sarasota Country, Fla., confirmed the concerns many had about e-voting, she had been planning legislation, similar to one that failed to pass in the House by two votes, mandating a paper trail for all electronic voting systems in the country. Electiononline.org's D. Chaplin said, "At first I thought there were lots of fender-benders on Election Day but no major pile-ups. But Sarasota is a pile-up." State officials and voting machine manufacturers are being pointed at to do a better job of testing and auditing equipment before elections. Republicans are pushing for legislation ensuring voter ID and fraud prevention, and Feinstein herself wants to outlaw state election officials from taking part in a federal candidate's campaign committee. Feinstein worries that continued problems, in a district that has greater national ramifications than Sarasota County, or worse, in a presidential election, will lead to a harmful loss of confidence in the nation's ability to conduct elections. Stanford University computer science professor D. Dill said lost votes complaints following the 2004 elections were not adequately investigated. He says, "The complaints need to be investigated urgently, or machine problems will lead to more disputed elections in the future."

Vote Disparity Still a Mystery in Fla. Election for Congress
Washington Post (11/29/06) P. A3; P. Whoriskey

Florida's 13th Congressional District is still trying to get to the bottom of why there were no votes cast for Congress by 18,000 Sarasota County residents who voted for candidates in other races. Some claim that the touch-screen voting system had a glitch that dropped votes, others that a confusing ballot caused voters to overlook the race, and finally that voters simply decided not to vote in this particular race, a possibility that has received little support. "Our analysis of the results show that something went very wrong," says K. Coffey, attorney for challenger C. Jennings, who is currently being declared the loser of the race, pending further investigation. Coffey dismissed a mock election that showed no signs of machine malfunction, in which clerical workers, not ordinary voters, used the machines to place votes. While 2.5% of voters did not cast a vote in every race in other Florida counties, a phenomenon known as "undervoting,"15% undervoted in Sarasota County. Two different election experts who had their own troubles with the voting machines support the theory that the machines are to blame, and the Sarasota Herald-Tribune reports over 100 reported problems with the machines. The confusing ballot idea is supported by the CalTech/MIT Voting Technology Project's director, MIT's T. Selker, who claims that his own tests show 60% of voters possibly missing races that are displayed in the way that the race in question was, but Coffey claims that such a high profile race is very unlikely to be simply forgotten or overlooked by so many voters.

DOD Report to Detail Dangers of Foreign Software
Computerworld (11/27/06), G. Anthes

The Defense Science Board (DSB), a military/civilian think tank within the Defense Department, has conducted a study into the security of software developed overseas, and will make recommendations to the DoD based on its finding, but will not advise that all military software be created within the United States. Chairman of the task force R. Lucky explains that, "The problem is we have a strategy now for net-centric warfare--everything is connected. And if the adversary is inside your network, you are totally vulnerable." The private sector has already experienced changes based on the task forces findings, although many see this attitude as simply xenophobia, stating that all software should be scrutinized equally. Lucky says that users should aim to make trade-offs between the amount of risk and the economics of creating a given piece of software. Protective steps cited by the DSB are: Peer reviews where several programmers review and test code; utilizing scan tools to search for hidden malware; and enforcing industry quality standards; and while each of these remedies is not a perfect fix or prevention, the combination will effectively "raise the bar," as Lucky says, and "eliminate a certain percentage of problems." However, those such as I. Winkler, author of "Spies Among Us," feels that a single line of foreign-written code contained in U.S. military software is too much a security risk. While such a policy would ideally ensure against foreign malware, there are few, if any, U.S. software companies whose products do not contain any code written overseas, and according to Lucky, "we're talking about complexity that boggles the mind. It's so enormous that no can truly understand a program with millions of lines of source code."

Canada Experts Find Path Round Internet Firewalls
Reuters (11/28/06), W. Dabrowski

People living in countries that overly restrict Internet access and block Web sites will be able to circumvent the firewalls of their government using new software developed by computer researchers at the University of Toronto. The program, Psiphon, is designed to turn an Internet user's computer essentially into a server that someone in another country can use to browse the Internet away from the watchful eyes of their government. Psiphon allows anyone living in a country that allows unfettered access to the Internet to set up their account, and then enable someone in a more restrictive country to log on from that computer. The free download, which will be available starting Friday, offers encrypted and secure Internet surfing for users, which will prevent their government from tracing their Web surfing patterns. "The communities that we're helping to connect to each other have a legitimate right to exercise their human rights within this government regime," says R. Deibert, director of the university's Citizen Lab, who also acknowledges that Psiphon might be unlawful in those countries. "It does conflict with some sovereign states' values, but there are competing legal norms at work."

Smart Spaces: If These Walls Could Talk
Computerworld (11/27/06), G. Anthes

The concept of "smart spaces" has been around for quite some time, and while the technology required for the individual components exists today, interoperability, accuracy, and reliability prove to be stumbling blocks. Different types of sensors, large touch-screen displays, cameras, microphones, and other devices were incorporated into a prototypical "interactive room," or iRoom, by Stanford researchers, which utilizes the Interactive Room Operating

System (IROS), a metaoperating system that they describe as having "taken the operating system idea to the space level, so people can coordinate their work in an environment with multiple devices," says Stanford computer science professor T. Winograd. The goal in such a project, as Winograd explains, is to maximize seamlessness and transparency, because, "Whenever you have to stop focusing on what you care about to focus on how the machine is doing, you lose fluency." IBM Research senior manager for responsive enterprise solutions S. Hild, who worked on an IBM prototypical interactive office, explains that, "The investment of taking an office building and enabling it that way is fairly high. But you can get 80% benefit with 20% of the cost." While such an investment could pay off, technology needs to make some progress first. Hild recognizes that turning an office building into a completely interoperable and interactive, real-time environment would require drastically scaling up networks and processors.