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

Δελτίο 51
8 Δεκέμβρη 2006

Security of Electronic Voting Is Condemned
Washington Post (12/01/06) P. A1; C. Barr

Electronic voting machines that were widely used in the past election "cannot be made secure," concludes a new National Institute of Standards and Technology (NIST) report. The report, which comes as the biggest blow to electronic voting from a federal agency, endorses optical-scan systems, stating that officials must be able to conduct a recount independently from the software on voting machines. Congress will hold hearings on NIST's report next week, but it will be up to the Election Assistance Commission to decide whether or not to adopt the recommendations. However, even if they do adopt them, the changes would not be fully implemented until 2009 or 2010. According to the report, the lack of a paper trail "is one of the main reasons behind continue questions about voting system security and diminished public confidence in elections." The report also echoes the concerns of many computer experts who warn that "a single programmer could 'rig' a major election," although there is yet to be any evidence of such activity. The alternative suggested by electronic voting machine manufacturers, of attaching printers to the machines, has met its own problems of printers jamming or simply failing, which prompts some, including VoteTrustUSA policy director W. Stewart to wonder, "Why are we doing this at all? We have a perfectly good system--the paper ballot optical-scan system".

Touch Screens? Vote Yes or No
Wall Street Journal (11/30/06) P. A4; J. Krunholz

Although most new electronic voting systems worked during the recent election, according to electionline.org, many changes are being contemplated in the way America votes. Sen. D. Feinstein (D-Calif.), who will take over as head of the Senate rules committee, and Rep. R. Holt (D-N.J.) have both proposed legislation to require paper records from touch screen voting machines, random audits of some of these records, and disclosure of the software code used in voting machines so it could be checked for vulnerabilities. Meanwhile, several states may take action to either abandon the new systems or modify how they're implemented. Cuyahoga County, Ohio, officials have announced that they are thinking of ditching electronic voting altogether and voters in Sarasota County, Fla., voted to return to paper ballots in the very same election where the votes of 18,000 citizens likely were lost due to problems with the electronic ballot. According to Election Data Services, over half of US counties used the money given by the Help America Vote Act to buy optical scan machines, while 36% bought touch screen machines. BYU's D. Magelby explains, that while voters do trust the touch screen machines, "it's a shaky trust." Those counties that want to change the way they vote now will have to pay for changes themselves. However, Congress could fund any changes mandated by federal legislation such as requiring a printed backup record of votes cast.

You're Not Alone
New York Times (11/23/06), W. Hamilton

As more aspects of the household become integrated into the Internet, the potential for damage done by hackers is increasing. Computer scientist P. Neumann, who specializes in security issues at SRI International, calls the home, "the next frontier of risk...here we are putting computer communications into the home so that [a hacker can] can turn on your oven, or overload your heating system...from anywhere in the world. You could bring down a lot of households simultaneously." The use of "botnets," groups of inadequately protected computers, often in homes, that hackers create into "armies" and sell to electronic criminals, has risen in the past year, and with 50 million homes now constantly connected to the Internet through broadband connections, the danger facing households is becoming greater. Symantec, in its annual threat report in September, stated that home computers make up 86% of those attacked, largely because unlike businesses, households don't realize the risk they face and therefore don't take appropriate security measures. Symantec's T. Powledge says that people don't realize how many devices in their homes are actually computers that can communicate with each other, and thus don't realize their potential to be exploited. Powledge says, "Your TiVo is a small computer, with an operating system, and all your devices can 'see' each other. When you have these kinds of devices that can communicate with other devices, the potential goes up that they can be exploited." Powledge notes that 80% of home network users don't activate the security features, while L. Rogers of CERT, Carnegie Mellon University's center for Internet security, says users don't want to have to worry about security in their home networks. Experts say the problem will only get worse as home theater systems are integrated with other entertainment services and the Internet and home automation systems take on health care, energy management, and other functions.

ACLU Urges U.S. to Stop Collection of Traveler Data
Washington Post (12/02/06) P. A5; E Nakashima

The ACLU, in formal comments submitted to the Dept. of Homeland Security, requested that the government end its data-mining efforts that examine every traveler entering or leaving the country. Begun as a cargo screening program by the customs agency, the Automated Targeting System (ATS) has been stepped up to establish "risk profiles" that will be kept on file for 40 years, meant to single out travelers who warrant scrutiny by customs officials. According to a Customs and Border Protection official, information has been collected on air passengers for the last 10 years, and ground passengers for the last 2 years. Electronic Frontier Foundation senior counsel D. Sobel said, "I don't see the logic of collecting massive amounts of information on millions of innocent citizens in the name of locating a small number of suspected terrorists. Casting that large a net raises issues both with respects to the security benefits as well as the privacy impact of the system." Customs spokesman P. Jones answered such criticism by asking, "How do they expect us to determine who's safe and who's at risk? We have over one million people coming into the country everyday." The customs agency plans to eventually enter data for all those who cross the borders, including name, date of birth, itineraries, and credit card information into its database. The agency explains that this wealth of information will allow it to construct models of travelers, both threatening and non-threatening

Nike+iPod Sport Kit Raises Privacy Concerns
University of Washington News and Information (11/29/06), H. Hickey

A device that allows runners to track their distance, speed, and amount of calories burned after a jog can also be used as a tracking device, without the knowledge of the person being tracked, according to researchers at the University of Washington. The kit consists of a small chip and a receiver that fits into an iPod Nano and collects data from the chip's movements. The small chip, designed to be slipped into a shoe, can be detected from 60 feet away, and the researchers were able to build devices that picked up and monitored this signal using a laptop or matchbox-sized computer with wireless Internet capability, the latter actually being able to show whereabouts of the chip on GoogleMaps. Decoding the unique tag on each receiver took the team about 10 minutes, and writing the code to interpret the information from the sensor took a few hours, but they guessed that someone with moderate knowledge of electronics could concoct a tracking system over a weekend, especially if the code were published online. The team imagined, and tested as best they could without infringing on privacy of others, scenarios such as a jealous ex-boyfriend who could hide receivers at locations that his ex-girlfriend frequents, in order to track her movements. Nike advertises the chip as something that can be dropped into a shoe and forgotten about, but the researchers urge users to remember to turn it off after a workout. Doctoral student in computer science and lead author of the technical report, which suggests ways the product could be made more secure, S. Saponas, explained, "It's an example of how new gadgetry can erode our personal privacy."