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

Δελτίο 72
2 Μάη 2007

Paper-Trail Voting Gets Organized Opposition
USA Today (04/23/07) P. 2A; R. Wolf

State and local officials have created a campaign to stop Congress from requiring a paper record of ballots cast on electronic voting machines, arguing such a requirement could create more problems in the upcoming elections. Groups representing secretaries of state, state legislators, and county leaders are cooperating in an effort to stop legislation scheduled for a House committee vote and Senate hearings. The legislation would require all electronic voting machines used in the 2008 elections to provide a paper record that gives voters proof of their vote that could be used as the official ballot in a recount. The legislation was expected to quickly move through the Democratic-controlled House, but committee action has been stalled and election officials claim the bill's requirements cannot be met in time for the presidential primaries in February. Election reform advocates support the bill, saying a paper trail, post-election audits, and other safeguards in the legislation cannot be postponed. Even without new federal legislation, the majority of the nation's voting machines will soon fail to meet the standards set by the federal Election Assistance Commission, particularly in regards to the requirements for assisting disabled voters. Most Republicans agree with election officials that the legislation creates too many requirements with too short a time frame to implement changes, but supporters of the legislation say objections will not slow the bill down. "There needs to be a paper trail," said Rep. Z. Lofgren, D-Calif. "If you can't have a paper trail, you can't do a recount."

Voting Machines a 'Catastrophe'--French Parties
Agence France Presse (04/23/07), M. Sailhan

Electronic voting has come under fire in France after widespread complaints of delays and problems with e-voting machines during the second round of the presidential election. The Socialists, the Communist Party, and the Greens called casting votes electronically a "catastrophe" in a statement, and nationalist Catholic candidate P. de Villiers referred to e-voting equipment as a "cheating machine." France is using e-voting machines for the first time, and about 1.5 million of the nation's 44.5 million voters used them during this stage of the election. Problems with e-voting machines in Paris suburbs prompted D. Guerin, a member of the Paris regional council, to lodge an official complaint with the Constitutional Council. Some voters said the machines were difficult to use, while others expressed concern about the secrecy of their ballot. An analysis of the vote also shows that four out of every seven voters 65 years of age or older were unable to record their vote. G. Michel, a psychologist who was involved in trials, considers e-voting to be a huge problem.

Nation's Cyber Plan Outdated, Lawmakers Told
Washington Post (04/26/07), B. Krebs; S. Mcloone

Plans and policies for securing the nation's critical online infrastructures are severely flawed and outdated, experts told lawmakers at a House subcommittee hearing on April 25. Practices such as report cards and policies addressing cybersecurity as an end rather than a means is

"procedurally correct but factually stupid," said biostatistician D. Geer in written testimony. J. Lewis, a security expert with the Center for Strategic and International Studies, told the Emerging Threats Cybersecurity and Science and Technology subcommittee that the nation's current cybersecurity strategy is outdated and has "shifted too much of the burden for security to the private sector and did not resolve key issues regarding responsibility within the government." Professionals for Cyber Defense President S. Saydjari provided written testimony urging lawmakers to start a $500 million "Cyber Manhattan Project" that would be run by the country's top experts, adding that preparing for cyber war will take more than three years and require infrastructure for critical computer systems, experienced defenders, and a national program. "The US is vulnerable to a strategically crippling cyber-attack from nation-state-class adversaries," Saydjari said. Lewis said that a new comprehensive strategy is needed to address issues such as how many interagency groups and committees are working of the same cyber issues, and also called cyber espionage the greatest current threat to the US. House Homeland Security subcommittee chair J. Langevin (D-R.I.) questioned the wisdom of funding cuts for HSD's science and technology directorate and questioned the administration's cybersecurity efforts.

Respectful Cameras
Technology Review (05/02/07), B. Borrell

University of California, Berkeley computer scientists have developed "respectful cameras," a new type of video surveillance technology that covers a person's face with an oval for privacy but removes the oval in the event of an investigation. Respectful cameras are still in the research phase, as they are only capable of covering someone's face if that person is wearing a marker such as a green vest or yellow hat, but the cameras could be a compromise between privacy advocates and those concerned about security, according to UC Berkeley computer scientist K. Goldberg. The researchers used a statistical classification approach called adaptive boosting to teach the system to identify the marker in a visually complicated environment, and added a tracker to compensate for the subject's velocity and other interframe information. When the system was tested using a vest at a construction site, the marker was correctly identified 93% of the time, and under more uniform lighting conditions while testing a hat in a lab, the system was 96% successful, even when two marked individuals crossed paths. Goldberg said the marker is necessary as face-detection algorithms are not advanced enough yet, but that a less conspicuous marker, like a button, could be used, particularly with systems of multiple cameras. Still, even if privacy protection camera systems were widely deployed, there likely would be debate on how difficult it should be for governments and law enforcement to see fully unobscured video footage.

Researchers: Health Sensors Open New Doors for Hackers
ASU Insight (04/30/07), D. Evans

A time when our health is constantly being monitored by a network of tiny sensors implanted in our bodies may not be as far off as some might think, according to S. Gupta, an associate professor in the Dept. of Computer Science and Engineering at Arizona State University. Not only does Gupta believe such a scenario could occur, but he has already considered the possibility that the "body sensor network" could be an information theft vulnerability. Like all other types of information exchanges, transferring information from tiny body sensors to a larger computer that interprets the data is vulnerable to theft and would need to be protected. Gupta has proposed a possible security solution using an algorithm based on a physiological property to generate a key to prevent unauthorized access. Using a synchronized measure-

ment of some phenomena in the body, a key would be generated simultaneously by two sensors so the key would never need to be sent between the two, keeping the key unknown to potential criminals. "This is a solution to the chicken-and-egg problem of secure data transmission," Gupta said. "Using the physiological parameters of the body, you can secure the information, and because the sensors are using their environment to derive the key, a person outside the body cannot measure the environment." While implant security is not yet a hot-button issue, Gupta says that as medical practices become more pervasive, specifically systems that use networks, security will become a critical issue.