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

Δελτίο 106
20 Φλεβάρη 2008

States Prepare for Tests of Voting-System Changes
New York Times (02/05/08) P. A14; I. Urbina

California's switch from touch-screen voting machines to paper-based ballots for Tuesday's primary has also brought back issues related to paper ballots, such as absentee ballots that fall apart at the fold lines and the ballot transportation helicopter being grounded by intense fog. "They may be high-tech or they could be low-tech, but the problems are always there," says B. Dunmore, the Riverside County registrar of voters. Election officials in at least 20 California counties without paper trails were told by the state to switch back to paper ballots, but the ballots will have to be counted at a central location where the absentee ballots are being counted because the counties were not able to acquire enough machines to perform tallies at individual polling places. All polling places in New Jersey, Delaware, and Georgia, as well as most of Tennessee, are using paperless touch-screen machines for their primary elections on February 5, and were considered "high risk" for voting problems before the election according to a report released by Common Cause and the Verified Voting Foundation. Experts say that meaningful recounts are impossible in a close race without a paper trail, and if problems occur with the voting machines, officials will be unable to audit contested results. Growing concerns about potential tampering or malfunctions have led election directors in Ohio, Florida, California, and Colorado to shift away from paperless touch-screen systems, but only California was ready in time for the February 5th elections.

Auditor's Report Inconclusive on Florida Undervote Mishap
Network World (02/08/08), G. Gross

The US Government Accountability Office still does not know what caused or contributed to 18,000 unmarked ballots in a Florida congressional race in 2006, the GAO said in a report released Friday. However, the report says that GAO's tests, along with others done by the state of Florida, "have significantly reduced the possibility that the iVotronic [machines] were the cause of the undervote." The GAO says that other factors, including intentional undervotes or ballot interaction problems, may have caused the undervote. The Verified Voting Foundation says the GAO report "leaves most of the major questions unanswered," and does not address potential problems with touch-screen sensitivity and low batteries, nor does it address reports of undervotes in other races. "The nature of the complex voting system in question, and the difficulty in auditing such a system, may mean such questions will remain indefinitely, but it is clear that more can and should be done to resolve the outstanding issues," a Verified Voting Foundation report says. The foundation suggests that auditors conduct more tests, including testing touch-screen sensitivity and checking for software bugs beyond the GAO's confirmation that the software matched Florida certification standards. "As someone who's interested in what happened in this election, my questions aren't answered," says foundation founder D. Dill. "I don't think we're going to get any idea about what happened in that election without a lot more investigation."

Web Browsing, Search, and Online Ads Grow More Risky, Google Says

InformationWeek (02/12/08), T. Claburn

Google security engineer N. Provos has found that Web browsing and searching are increasingly becoming channels for the distribution of malware. Provos says that more than 1% of all search results in the past few months contained at least one result that was believed to point to malicious content. He says that in the 18 months that Google has been tracking malicious Web pages, the company has found more than 3 million unique URLs on over 180,000 Web sites that attempt to install malware on users' computers. A recent paper Provos co-authored with Google colleague P. Mavrommatis and Johns Hopkins University computer scientists M. Abu Rajab and F. Monrose blamed the problem in part on Internet advertising, Google's main source of revenue. Provos found that an average of 2% of malicious Web sites were delivering malware via Internet advertising, based on an analysis of about 2,000 known advertising networks. But since Internet ads target popular sites, search engine users are more likely to find them than that statistic suggests. The report noted that an average of 12% of overall search results that returned landing pages were associated with malicious content due to unsafe ads. Provos says there are no readily-apparent solutions to the problem.

Workplace Autopilot Threatens Security Risk Perception
University of Leeds (02/08/08)

Human psychology and the way we perceive risk make it impossible for organizations to completely secure their data, no matter what preventative steps they take, concludes research conducted by Britain's Leeds University Business School. During the study, people who regularly used IT systems at work were asked to list examples of possible data security risks, either imaginative or ones they have seen in their personal experiences. Another group was asked to comment on the probability, underlying causes, likely consequences, and impacts of the scenarios that were most commonly listed. The study found that many of the risk examples listed by the participants matched recent security breaches, despite the fact that the survey data was collected over a two-year period. Professor G. Hodgkinson, director of the Center for Organizational Strategy, Learning, and Change, says the research shows that organizations will never be able to remove all of the latent risks in the protection and security of data stored on IT systems because people's brains naturally run on "automatic pilot" in routine situations. R. Coles, the study's co-author, says the results of the study show that employees exhibit a highly-sophisticated perception and categorization of risk, as well as insight into the consequences of risk scenarios, when asked to focus on potential problems. But since this perception is not always translated into practice, errors are still happening and will continue to happen in the future, Coles says.

Wearable Tracking Tags Test Privacy Boundaries at the U. of Washington
Chronicle of Higher Education (02/15/08) Vol. 54, No. 23, P. A15; R. Dotinga

Determining the effectiveness as well as the appropriateness of tracking people through radio-frequency identification (RFID) tags is the goal of the University of Washington's RFID Ecosystem project. Researchers have installed 140 antennas and 35 RFID readers to monitor areas of the P. Allen Center for Computer Science and Engineering so that between 100 and 150 computer-science students, faculty, and staff members can eventually track people--and can themselves be tracked--on the project Web site. The objective of the effort is to "create a future world where RFID's are everywhere," says computer science professor G. Borriello. The idea is to analyze the choices participants make in terms of when and how frequently they monitor their own and other people's activities, and what information they wish to acquire. Monitoring is not allowed in certain areas of the building--such as restrooms--in order to prevent RFID surveillance from becoming too intrusive, and participants will be allowed to control who can view data about their movements and even instantly exit the network. University of Washington graduate student E. Welbourne says the point of this exercise is to ascertain whether people will tend to opt in or opt out. He says that so far the project has concluded that "technology itself is not an inherent risk to privacy, or at least not in any way that can't eventually be fixed." An earlier experiment at the University of California at San Diego involved students tracking each other's whereabouts via Wi-Fi-enabled PDA and professor W. Griswold notes that some students elected not to be monitored while others broadened the level of access to their locations.