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

Δελτίο 48
19 Νοέμβρη 2006

Glitches in State Databases Could Turn Away Voters
Computerworld (11/06/06), M. Songini

The November 7 elections will mark the first use of a centralized voter database in a general election in Florida and many other states. These databases are governed by state selection officials in accordance with the Help America Vote Act. However, the databases require that new-voter information match information in other databases, such as the Dept. of Motor Vehicles, says D. Wheatley-Giliotti, president of the League of Women Voters of Florida (LWVF). The databases were compiled quickly, providing IT workers minimal time for proper training. Leon County, Fla., has the benefit of having previously used a database system on which the new system was built, so IT personnel there will be better prepared, but according to I. Sancho, head of elections for the county, "Other counties don't know all the ins and outs." Discrepancies, such as "Bill" in one database and "William" in another, would mean that this voter would receive a provisional ballot, and would need to furnish proper documentation within three days; contrary to the belief of many that a voter in this position would simply be sent home, says a spokeswoman for Florida Secretary of State S. Cobb. Some ineligible voters have been sent warnings, but many will find out at the poll site. J. Levitt, associate counsel with the democracy program at New York University School of Law's Brennan Center for Justice, cites Ohio's eligibility practices that are quite unclear, explaining, "Where the systems are less transparent, there's greater reason for concern." The provisional ballot is meant to assuage voters' fears concerning ineligibility, but LWVF's W. Giliotti sees it as yet another obstacle for a shrinking pool of voters to negotiate.

E-Voting, As It Advances, Faces Big Risks
Baseline (11/03/06), R. Hertzberg

The Defense Department's Interim Voting Assistance System is the latest electronic voting initiative to come under fire from critics who are concerned about voting security risks. Former ACM President B. Simons criticized IVAS in a paper in late October, questioning whether the complex program was hastily put together from June 15 through Sept. 1. Simons is also concerned about the Pentagon's decision not to implement encrypted email for the system. Having overseas military personnel send their votes via unencrypted email could make soldiers victims of identity thieves or hackers and foreign governments who want to tamper with the vote count. "I'm personally offended that people who are fighting and dying for our country are being told they have to give up their right to vote in secret," she says. Meanwhile, Simons says the security measures implemented by e-voting system manufacturers such as Diebold Election Systems will not be enough to safeguard elections because the companies are only addressing problems they know about. She says, "You can fix the problems you know about. But somebody's going to attack you at your weak point, on something you haven't thought about."

E-Voting: Dispatch From the Future
Washington Post (11/05/06) P. B1; W. Dreschler

Estonia conducted the world's first nationwide online election on October 16, 2005, which came off without a hitch. Ever since claiming independence following the 1991 collapse of the Soviet Union, Estonia has been dedicated to integrating technology into society, including chip-based ID cards with digital signatures carried by citizens and more sophisticated e-banking system than the US. The rate of Internet use is 60%, compared with 70% in the US. Voters had the choice of voting over the Internet, or actually coming to the polls, and online voters were given the option of a paper ballot in order to confirm their vote. Only 2% of voters did so online, yet the Reform Party, whose members are considered the most tech-savvy, did better among online voters than traditional voters, while the less tech-savvy Center Party did better among traditional voters. The only problem encountered was the need for e-voters to buy an ID-card reader (about $15) and install it using software that many found difficult to use. Estonia is planning to use e-voting in its 2007 parliamentary elections. Although the option of voting over the Internet did not appear to boost voter turnout in Estonia's election, it's likely that the parties that attract more tech-savvy users will benefit, a fact that has implications as more and more countries inevitably move to e-voting in the future.

Watchdog Groups Report E-Voting Problems
IDG News Service (11/07/06), G. Gross

Election watchdog groups across the US received reports of e-voting problems during the November 7 election. Over 1,4000 calls had been received by Common Cause by 4 pm EST, including hundreds of reports of vote flipping that were caught on the machine's summary screen. Verified Voting, another watchdog group, called for a national investigation into vote-flipping after the 2004 election, but this request was denied. D. Dill, founder of Verified Voting and a computer science professor at Stanford, said, "Not surprisingly, we are expecting the same problems...I think it's a national disgrace." However, Common Cause received fewer e-voting complaints than after the 2004 election, although Dill claims that many complaints are yet to surface. Denver voters had to wait in hour-long lines at the polls as a result of a plan to let people vote wherever they wanted. A single, overloaded database held all of the voter rolls: "It's the classic situation where too many cars are jammed onto one highway," said P. Naismith of Common Cause Colorado. Other problems reported, according to Common Cause, the Election Protection 365 Web, and ACM, include: 43 of Cuyahoga County, Ohio's 573 polling places opened late or couldn't get some voting machines to work. A judge ordered 16 polling places to stay open an extra 90 minutes; in one Indiana county, machines failed to turn on, and in a second county machine activation counts were not programmed correctly; and other problems were reported in Pennsylvania, Utah, and Florida.

'Vote Flipping' Emerges as Continuing Problem in E-Voting
Computerworld (11/08/06), T. Weiss

The problem of "vote-flipping," originally reported during the 2004 election, emerged once again during Tuesday's general elections, as watchdog groups received many calls from voters reporting that their votes did not appear on the electronic voting machine's summary screen as they had been entered. D. Dill, computer science professor at Stanford called for investigation into these claims. "People have been way to quick to diagnose the problem," he said. Some have blamed the problem on calibration, but others have ideas of their own. "It could be a calibration problem with the touchscreens, but I'm no sure that anyone really knows yet because no one's looked at it," added Dill. "My answer as a computer scientist is that I want facts...and all I've heard for two years is speculation." Dill believes that the summary screen shows that conspiracy is not likely. One suggestion he made was that voters may

accidentally touch the screen inadvertently and not realize they have selected a candidate, but he feels that a panel of experts must be convened to get to the bottom of whatever the problem may be. "There needs to be a serious independent investigation of this problem... across the country," he said. Precinct-scan optical scan ballots, which are filled out by the voter and read by a machine, are the method preferred by Dill, since they give a voter written confirmation, providing a paper trail.

Inside the Hacker's Profiling Project
NewsForge (11/03/06), F. Biancuzzi

The Hacker Profiling Project (HPP) has set out to combine criminology and ICT security science in an effort to use information left by hackers on compromised Web sites to gain an understanding of specific hackers so future attacks can be prevented. Alerting potential victims to the type of threat they face will allow system administrators to take proper defense measures, explains S. Ducci, criminologist for United Nations Interregional Crime and Justice Research Institute. By both circulating a questionnaire among members of the hacker underground known not to be professionals, and setting up honeynets that will register and collect information regarding attacks and movements of hackers trying to penetrate their systems, HPP expects to gain a greater understanding of different types of hackers. The questionnaire is divided into personal data, relationships (to other hackers, colleagues, authorities, etc.), and technical and criminological data. Many of those expected to answer the questionnaire practice hacking in their spare time, and many are considered "ethical hackers" that will often alert sysadmins to vulnerabilities on violated systems, although this information is often shared with others in the hacker community as well. HPP wants to be able to construct a profile of attackers including "technical skills, probable geographic location, an analysis of his modus operandi, and a lot of other, small and big, traced left on the crime scene," says Ducci. She envisions the project yielding a complete, open "methodology for hacker profiling, released under GNU/FDL."

'Vote Flipping' Is Real, But Its Cause Is the Subject of Debate
Computerworld (11/13/06), T. Weiss

Voters in several states said during last week's election that electronic voting machines counted their vote for the candidate they did not select. Charges of "vote flipping" were made in the 2004 elections as well, but the cause of the problem remains unknown because the issue has not been studied. Some opponents of e-voting maintain that the problem is caused by e-voting machines, but other observers say vote-flipping could be the result of voter error or machine calibration. Experts who believe user error is the problem, such as Voting Technology Project co-director T. Selker, say voters are dragging their fingers across the touch screens instead of tapping their selection, which is resulting in their choice of the wrong candidate. Machine calibration could be a contributing factor as well, and Rice University computer science professor D. Wallach says e-voting machine vendors may need to make bigger selection buttons and create more distance between them on the screen. Stanford University computer science professor D. Dill, who rules out a vote defraud conspiracy, says the issue needs to be investigated. "I want facts...and all I've heard for two years is speculation," he says.

ACM Group Honors Computer Security Experts
AScribe Newswire (11/08/06)

ACM's Special Interest Group on Security, Audit, and Control (SIGSAC) presented its top honors to Michael Schroeder of Microsoft Research and Eugene Spafford of Purdue University during the Computer and Communications Security Conference in Alexandria, Va., last week. Schroeder received the SIGSAC Outstanding Innovation Award for his contributions to the Needham-Schroeder authentication protocol, which is used in many commercial security products today. Industry standards are based on Needham-Schroeder, the protocol that provides mutual authentication for two parties communicating over a network that is not secure. Schroeder was named an ACM Fellow in 2004, while Spafford was named one in 1998. The computer science and electrical and computer engineering professor received the SIGSAC Outstanding Contributions Award for his participation on a number of national panels that helped set the US cybersecurity policy. Spafford, also the chairman of the ACM's US Public Policy Committee (USACM), most recently served on the President's Information Technology Advisory Committee (PITAC) in 2003-5.

Ballot Roulette
Science News (11/04/06) Vol. 170, No. 19, P. 298; Weiss, Peter

Improved methods for voting reliably and securely are being investigated by mathematicians and computer scientists whose forte is encryption. Simplifying programs used in touch-screen voting systems is one method proposed by a research team at an August voting-technology meeting in Canada; the process involves the election officials mocking up all possible ballot screens in advance, and having the voting machine display the screens and record voters' responses on Election Day. A second research team suggested that an election district's central computers could be made more secure by a cheap device that stops incoming messages, permitting data to move only from the secure election machines to the outside. Harvard University's B. Adida and MIT's R. Rivest have designed a cryptographic voting process, Scratch & Vote, that uses paper ballots to enable voters to check that their votes were properly recorded while also allowing observers to test the accuracy of the vote tallying without infringing on voter privacy. Scratch & Vote involves the use of a perforated ballot with voting boxes on one side and candidates' names on the other; once a ballot is marked, each voter removes and destroys the portion with the candidate names, and then feeds the other portion, which has an encrypted version of the names and the order in which they are arranged, into an optical scanner that records the vote. The voter retains that portion as a paper receipt, offering incontestable documentation of the ballot. The Punchscan cryptographic method, meanwhile, features scannable ballots with a pair of layers that voters mark with ink daubers. Either layer can be kept by voters without revealing their selections.

Sensor Networks Protect Containers, Navigate Robots
Washington University (St. Louis) (11/09/06), T. Fitzpatrick

Researchers at Washington University in St. Louis have achieved a new level of flexibility in wireless sensor networks, which can support multiple applications over the same hardware to meet changing conditions. In an experiment, a sensor network that utilized software agents was able to locate a simulated fire and direct a robot to the location, using heat detection. After finding the fire, the software agent "clones" itself, forming a ring of software around the fire that a fireman can use to learn about the fire, and if the fire grows, another ring can be created. The research team created a middleware program called Agilla that allows agents to traverse sensor networks connected through the Internet, creating intricate communities of agents in cooperation. G.-C. Roman, the H. and A. Welge professor of Computer Science and department chair, and director of Washington University's Mobile Computing Laboratory,

who contributed to the project, predicts that wireless sensor networks are ready to have a huge global impact, not unlike the rise of the Internet following the development of the World Wide Web. "What researchers are banking on is that sensor networks will be so cheap to make that they can be employed on a very large scale," says Roman. "This way you can spread hundreds and thousands of them around gathering data and communicating." Potential future applications include a farmer retrieving data concerning the various types of soil on his land, or a warehouse monitoring its containers.

Researcher Finds 'Trusted Computing' Chip in Apple Models
eWeek (11/10/06), D. D. Turner

A "trusted computing" module (TPM) was found in Intel-based Apple computers, but the reason for it is unknown. A. Singh, a member of Google's technical staff, discusses the existence of the chip in his book, "Mac OS X Internals: A Systems Approach," in which he also writes that there is no way for Apple's Mac OS X to directly make use of the TPM; no DRM or similar restrictions are linked to the chip. "The TPM is an opt-in feature," said Singh. "Apple can't turn it on--nobody can, other than the user." The TPM is a single chip that is made up of a random number generator, a small memory chip, and a low-power processor, plus a few other parts. It has no influence on the system due to a lack of drivers that are aware of it in either the computer's OS or its firmware. While it is possible for users to make use of the TPM, Singh's best guess is that the chip is simply part of the motherboard package from Intel. R. Anderson, a professor of security engineering at the Computer Laboratory at the University of Cambridge, does not believe that the TPM would be included without reason. Based on "software economics" and "Apple's traditional business model," he suggests "future use of the TPM, whether in OS X 10.5, 10.6 or later," or "use directly by application software vendors, e.g. in Office 2007." Anderson has been very critical of past trusted computing efforts, linking them to attempted, strict DRM restrictions, such as the prevention of the copying of purchased media files or the playing of a CD on more than one computer.