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

Δελτίο 54
28 Δεκέμβρη 2006

Paper Jams a Problem for Electronic Voting, Associated Press (12/21/06), S. Manning

Paper jams have emerged as a major problem for the "paper trail" e-voting strategy that was advocated by many experts as a way to ensure a means of independent verification for electronic voting. Johns Hopkins computer scientist A. Rubin points out that the flaws only exist in the current paper trail system and that the idea should not be abandoned: "This isn't what we had in mind when we called for paper. I have yet to see a paper trail system I like." In an audit of its paper records, Cuyahoga County, Ohio, found that the manual count did not match the computer-tallied results because 10% of ballots were either smeared, torn, crumpled, or blank. Machines also jammed in California, Mississippi, and Missouri. In North Carolina's Guilford County, an audit of a sample of voting machines revealed that 9% of printers either malfunctioned or had paper problems. "How many votes were lost as a result of that, with the printer chewing it up?" asked G. Gilbert, elections director for the county. "If you don't have a complete paper record, you can't use it for a recount." Diebold's D. Bear says the problems with the company's machines were the fault of election workers. He says, "The technology has proven itself in thousands of elections." Some states that adopted touch-screen voting systems with no paper trail are now questioning the current drive for optical scan machines, claiming that the idea behind recent election changes was to get away from paper, as well as citing the high cost of replacing a relatively new system.

How Biometric Security Is Far From Foolproof, Wall Street Journal (12/21/06) P. B3; M. Bulkeley

As more businesses begin relying on biometric security devices, many wonder how susceptible they are to fakery, and their fears may be justified. International Biometrics, a consulting firm, was hired by a New York-based financial group to look into the plausibility of such "spoofing." Most fingerprint scanners simply take a picture of the fingerprint and compare it to those in a database, so "any high-resolution image will have a high chance of spoofing an optical sensor," says International Biometric's R. Mitchell. Systems employing non-optical sensors, such as thermal or ultrasonic, could be less vulnerable, but vulnerable nonetheless. West Virginia University researchers claim to be able to fool various types of fingerprint readers between 40-94% of the time, using fingers from cadavers or made of Play-Doh, and T. Matsumoto, a Japanese mathematician at Yokohama National University, claims to have fooled readers using fingerprints made out of gelatin. Manufacturers downplay security threats, citing that most successful spoofs involve molding an actual fingerprint, which would be very difficult for a criminal to obtain, and that making a replica of a fingerprint on a piece of glass is extremely difficult as well. However, Mitchell believes that even the most advanced biometric readers, "despite high matching accuracy, could be fooled using cheap materials." Although iris recognition technology being developed is a more secure form of biometrics, it too could be fooled using a high-resolution photo, so developers are working to overcome that by attaching a light that would contract the pupil and prove that the eye is real.

Justice Dept. Database Stirs Privacy Fears, Washington Post (12/26/06) P. A7; D. Eggen

A huge database being constructed by the Justice Department intended to allow local investigators around the country to access information held by federal law enforcement agencies is receiving widespread disapproval from privacy groups. There are currently one million records, from both open and closed cases, in the database known as "OneDOJ," which can only be accessed by 150 police departments at this time, but in three years the number of case records is expected to triple, and the number of regional authorities with access is expected to jump to 750. Privacy and civil rights advocates see the database as a dangerous source of unfounded details, particularly concerning people who have not been arrested or charged with a crime. The ACLU's Technology and Liberty Project director B. Steinhardt says that, "Raw police files or FBI reports can never be verified and can never be corrected. That is a problem with even more formal and controlled systems. The idea that they're creating another whole system that is going to be full of inaccurate information is just chilling." He cites the 2003 statement by the FBI that it would no longer recognize the Privacy Act's requirements for accuracy in the National Crime Information Center, the main criminal-background-check database that is utilized by 80,000 law enforcement agencies in the country. Others express fear that the information disseminated by this system could make its way into realms outside of law enforcement. Despite calls for a halt to the project, the DOJ remains confident that One-DOJ will provide invaluable assistance to local authorities by "essentially hooking them up to a pipe that will take them into [the DOJ's] records."

Congress in 2007: Privacy, Patents on Agenda, IDG News Service (12/22/06), G. Gross

The newly elected Democratic Congress has raised the hopes, and fears, of many involved in the tech industry, as several issues that had died on the floor are expected to be brought back to life in 2007. In late 2005, Microsoft joined privacy advocates in demanding data protection standards and personal data-privacy legislation, and as the issue becomes more prevalent, cybersecurity vendors and others will renew a focus on this concern. The conflict will continue between large companies that wish to put an end to what they call patent "trolls," whom they accuse of applying for patents then claiming infringement strictly for profit, and the independent inventors and programmers who claim they rely on current patent laws to make a living. In December, the FCC voted to strip down the process by which broadband providers gain permission to offer IP service, which may take some energy out of the telecoms' support for wide-ranging broadband reform. Verizon has announced that it will focus on state legislation and FCC rule making, rather than Congress. Net neutrality will surely be an issue, but Republicans could use the same tactics to stall a Net-neutrality bill that Democrats used to prevent a broadband bill this year. An increase in the number of H-1B visas granted will be strongly pushed by tech companies, as the 2007 cap was reached two months before the fiscal year even began. Debates over illegal immigration caused such bills to stall last year, and now it seems that the hiring of H-1B workers for less than prevailing US wages will cause a push for a complete reform of the system. The H-1B program was not mentioned by N. Pelosi in her "first 100 hours" plans, and many predict that the new attitude of controlled spending taken up by Democrats will cause a loss of interest in the program.

Voter Paper Trail Not an Easy Path, Atlanta Journal-Constitution (12/22/06), C. Campos

An examination of the much discussed e-voting paper-trail audit system used in several Georgia districts revealed that the process is far from a silver bullet. The paper-trail solution gained popularity in the wake of many warnings from computer scientists that e-voting machines were vulnerable to tampering. Cobb County, Ga. head of elections Sharon Dunn recent-

ly testified in front of state officials, who are considering making paper-trials mandatory in all of the state's voting districts, regarding the effort needed to manually count the 976 printouts generated in the district: Twenty-eight people took part in the five-day task of counting the votes from 42 races, and teams often had to restart their counts as numbers did not match up. Dunn testified, "It looks easy until you have to do it." Other issues raised included how printouts would be stored, whether or not they would be considered official ballots, whether volunteers, often elderly, would be capable of dealing with the technology, and the likelihood of printer malfunctions. MIT political science professor specializing in elections C. Stewart said, "Audits ask humans to do something that computers are generally better at doing."

PHP Security Under Scrutiny, Security Focus (12/18/06), R. Lemos

Web applications written using PHP tools have proven to be difficult to protect. Nearly 20 million domains and 1.3 million IP addresses that host Web sites now use PHP, according to Netcraft's October 2006 survey. However, a search of the National Vulnerability Database, which is maintained by the National Institute of Standards and Technology, recently revealed that Web applications written in PHP likely made up 43% of this year's security problems, an increase from last year's 29%. NIST senior computer scientist P. Mell, the program manager for the vulnerability database, says that although PHP's security issues are partly due to the language itself, many are due to how developers implement the language. Nevertheless, he says, "In the dynamic programming language (and) scripting realm, we certainly have a problem. Any time a third or more of the vulnerabilities in a given year are attributed to a single language, you know you have a problem." Security researchers say hackers are increasingly focusing on the vulnerabilities in Web applications; researcher S. Christey says database injection bugs, PHP vulnerabilities, and cross-site scripting flaws, all Web application flaws, were the three most common flaws in the first nine months of 2006. The PHP Group says it has worked to accommodate less-savvy developers by making the language more foolproof. PHP Group Z. Suraski says, "We have shown in the past that we are willing to change defaults and sometimes to remove features, just to make it more difficult for developers to make security mistakes." Still, Mell says writing secure code is challenging, even for professionals, and needs to be made "dummy proof." He says, "I think it is tough for the general public to write secure dynamic Web applications."