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

Δελτίο 15
17 Μάρτη 2006

Md. House Approves Paper Ballots
Washington Post (03/10/06) P. A1; A. Marimow, Y. Woodlee

In a unanimous vote, the Maryland House of Delegates endorsed the use of paper ballots in its next election, scrapping the state's touch-screen machines in a move supported by Republican Gov. R. Ehrlich that represents an about-face for a state that had been at the forefront of touch-screen voting technology in 2001. Under the plan, the state would lease optical ballot machines for $13 million, while the $90 million touch-screen machines would be shelved for one year. It remains uncertain how the plan will fare in the Senate, and there is no money in Ehrlich's budget earmarked for the new machines. Diebold will demonstrate for lawmakers an updated version of its touch-screen system that produces a paper record. The challenges that Maryland has had in selecting a voting system are typical of the pains that election officials feel nationwide as computer experts question the reliability and security of touch-screen systems. Voter verification is now required in more than two dozen states as advocacy groups have lobbied to ensure that voters can have confidence in the accuracy of their ballot. Within Maryland, some officials have argued that optical scan machines are a step in the wrong direction, given that the hand-marked ballots can produce ambiguous results. "There is no evidence of anything wrong with Maryland elections," said J. Willis, the former Secretary of State, pointing to the study conducted by the California Institute of Technology and MIT that identified Maryland as the state with the lowest voter error in 2004. ACM's US Public Policy Committee has issued a report on "Statewide Databases of Registered Voters: A Study of Accuracy, Privacy, Usability, Security, and Reliability".

FCC Brief on Electronic Surveillance Calms Colleges' Fears About Costs
Chronicle of Higher Education (03/10/06) Vol. 52, No. 27, P. A30; A. Foster

The FCC has filed a brief with the US Court of Appeals for DC that could be good news for colleges in the US who feared thy would have to spend an average of $9 million to $15 million each to comply with an FCC post-9/11 mandate that broadened the Communications Assistance for Law Enforcement Act to allow federal monitoring of broadband networks and Internet-based telephone services. Originally, colleges thought they would have to overhaul their entire networks, replacing every router and switch so emails originating from within and without campuses and those moving between students and staff could be intercepted. But the FCC, in its brief, says only those emails flowing in and out of campuses, and not those moving within, would be monitored, necessitating modification or replacement only of equipment that connects college networks to the Internet, according to one school of thought. The FCC's original mandate was challenged in court by the American Council on Education, eight post-secondary education groups, and two academic library groups, as well as others.

Aggregated Information Threatens Privacy
Norristown Times Herald (PA) (03/13/06), K. Phucas

Technological advances have enabled the federal government to increasingly gather and search American's personal information, says the American Civil Liberties Union, who also no-

tes that the government often purchases individuals' personal information that it cannot obtain legally from data aggregating companies. The ACLU warns that Lexis Nexis, ChoicePoint, and others have built a multi-billion-dollar industry out of the increased demand for personal information and lax privacy laws, while the information collected and shared often contains glaring inaccuracies, such as erroneous criminal records. The federal government was running 131 data mining initiatives in 2004, with plans to launch another 68, according to the Government Accountability Office. The Verity K2 Enterprise, a Defense Intelligence Agency initiative to search for terrorists overseas with connections to U.S. citizens, is particularly controversial. A Freedom of Information Act request filed by the Electronic Privacy Information Centre to obtain disclosure of the initiative's activities was denied, and the centre has followed up with a lawsuit. DIA spokesman Don Black reported no knowledge of the program, but said the agency routinely runs comparative analyses on terabytes of data, likening its activities to Google. Black also said the agency always looks for something specific in its searches. The ACLU has also warned of the numerous government contracts held by data aggregators (ChoicePoint has 35) that enable the government to skirt the requirements of the Privacy Act of 1974 prohibiting the government from compiling data about its citizens who are not the subject of investigations. Data collection is subject to a host of complex and often vague laws, which could be streamlined so that other companies would have to follow the rules of Internet service providers, who are not allowed to store customer information permanently, according to Villanova law professor M. Carroll.

Research on the Road to Intelligent Cars
IST Results (03/09/06)

The IST-funded PReVENT program, a component of the European Commission 2010 Intelligent Car Initiative, is attempting to develop new safety applications in cars that will sense danger in an effort to meet the EU's goal of cutting the number of highway fatalities in half by 2010. While high costs and lack of demand stymied earlier attempts to include intelligent safety systems in cars, the technology exists today to deploy them inexpensively and on a wide scale. A dashboard display in a BMW creates digital maps with lasers and sensors to extend the driver's horizon by 300 meters to 500 meters, allowing him to anticipate what is coming around the next curve. MAPS&ADAS project partners will submit the technology for certification, and auto makers hope say the new interface could lower the cost of implementation. The project is also working to make digital maps into more than just navigation devices by incorporating information on speed limits, slopes, curves, and traffic signs to improve their use as a safety application. Project leaders expect to see the results of the initiative appear widely in cars within five years. Another PReVENT subproject, INTERSAFE, is focusing on improving traffic safety at intersections, which pose the greatest challenge to a car's onboard sensors. The INTERSAFE project is developing new vehicle localization algorithms, sensors to warn of approaching drivers, and new techniques for communication between the road and the vehicle. The system is particularly designed to help drivers when they miss stop signs and red lights, make left turns, and cross traffic. APALACI, another sub-project, is developing applications to prevent and mitigate crashes, such as tightening seat belts immediately before a crash and preparing a car's brakes to avoid an accident. "The challenge for intelligent safety systems is to avoid false alarms, so that users quickly come to trust them," said Daimler Chrysler's M. Schulze.

Open Source Software Capability Key to 'Technological Self-Determination'
LinuxElectrons (03/08/06)

Experts from the United Nations University herald open-source software as a tremendous opportunity for developing nations to obtain economic independence, but also warn of the critical need to cultivate local expertise to support open-source development. Between 50% and 75% of Internet activity involves open-source software, and UNU experts believe that China, East Asia, India, and South America will be the largest markets for open-source solutions, though there remains a shortage of developers. "Should this situation persist, developing nations will simply remain consumers of open-source products rather than participants in the larger open-source market," says Mike Reed, director of the UNU International Institute for Software Technology (UNU-IIST). Open-source technology provides a framework that enables enterprises to develop high-value products more quickly, a key ingredient in the transition from passive consumer to active participant. Within the Linux environment, analysts predict that revenue from packaged software will grow the fastest, increasing 44% annually over the next four years. Open-source development will benefit the governments of developing nations as well as industry, providing low-cost implementation of local solutions and content, and greater standardization and transparency. Open source has also enabled governments to develop innovative solutions in a host of areas, including customs reform, providing online access to land titles, and electoral reform. UNU-IIST is attempting to increase the number of open-source developers in East Asia through the Global Desktop Project, aimed specifically at improving the open-source desktop. The project includes a research and engineering component, an institute of higher learning program, the incorporation of open-source programming into school curricula, and a community outreach program.

Scientists Band Together for TRUST-worthy Research
SearchSecurity.com (03/07/06), N. McKay

The Team for Research in Ubiquitous Secure Technology (TRUST) initiative is performing a key role in the nation's effort to safeguard its digital infrastructure from cyber criminals. Funded by $19 million from the National Science Foundation, and led by the University of California, Berkeley, TRUST brings together computer security leaders from universities across the country to build better systems and develop better policies for government and business. In fact, policy changes can determine the effectiveness of technology, particularly with regard to the use of publicly available information such as Social Security numbers to partly authenticate an individual, according to F. Schneider, chief scientist of TRUST. Schneider, who is also a professor of computer science at Cornell University, adds that storing large amounts of information on individuals, often without their consent or knowledge, is another issue that needs to be addressed as a matter of policy. Among other projects, TRUST participants are focusing on language-based security to develop "security grammar" for computer programming languages, as a way to warn systems and users before they run software executables and worms downloads. Participants from Stanford University have developed software for the US Secret Service called PwdHash, which is designed to prevent a cyber attacker from intercepting messages in a public key exchange and substituting his own for the requested one. Experts from Carnegie Mellon, San Jose State, and Vanderbilt universities and several small liberal arts colleges are involved in TRUST, which is also receiving assistance from companies such as IBM, Cisco Systems, and Microsoft.

Study Says Chips in ID Tags Are Vulnerable to Viruses
New York Times (03/15/06) P. C3; J. Markoff

A team of European security researchers has shown that radio frequency identification (RFID) tags contain a vulnerability that a hacker could exploit to transmit a software virus by

infecting even a small portion of the chip's memory. The researchers, associated with the computer science department at Vrije Universiteit in Amsterdam, warn that in addition to the host of privacy concerns raised by the widespread use of RFID tags, the newly discovered vulnerability could enable terrorists or smugglers to pass through RFID luggage scanning systems at airports. The researchers tested software intended to replicate the commercial software in RFID tags, and noted that while they did not have a specific flaw to report, they believe that commercial RFID software contains the same potential vulnerabilities that can be found in the rest of the computer industry. The group's leader, American computer scientist A. Tanenbaum, warned specifically of the dangers of buffer overflow, a common programming error throughout the software industry where developers fail to verify all of their input data. The low cost of RFID tags, the critical feature that enables their widespread deployment in tracking cargo, merchandise, and even livestock and pets, is also a security concern, according to SRI International's Peter Neumann, co-author of a forthcoming article in the May issue of the Communications of the ACM. "It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever," Neumann said, citing the potential to counterfeit or deactivate tags, insufficient user identification, and the poor encryption of the US passport-tracking system under development, though he had not previously considered the possibility of viruses or malware.

Judge Says Google Must Hand Over Search Records
Washington Post (03/15/06) P. D1; Y. Noguchi

US District Judge J. Ware yesterday ordered Google to turn over thousands of Web search records to the Justice Department, which marks a turning point in a case where Google refused to release such information in accordance with a federal subpoena on the grounds that it would expose its trade secrets and jeopardize Google's protection of users' privacy. Ware felt Google faced less of a burden since the government has narrowed the scope of the original subpoena from a random sampling of 1 million Web sites and a week's worth of search queries to only 50,000 sites and 5,000 queries, and is willing to reimburse Google engineers for the work such a request entails. Google general counsel N. Wong stated that Ware's comments "reflected our concerns about user privacy and the scope of the government's subpoena request. At a minimum, we've come a long way from the initial subpoena request." The Justice Department wants the information it requested from Google and other online search services to build a case that the Child Online Protection Act is constitutional, and prove that filtering software cannot effectively limit minors' access to Internet pornography. The government insisted that it is not looking for personally identifiable data about Internet users, but privacy proponents are concerned that the government might go too far in tracking online activities. "It's really about the outsourcing of surveillance to these private companies, and the question is: How legitimate is that?," notes Seton Hall University School of Law professor F. Pasquale. Still, a new Ponemon Institute poll finds that Americans are more worried about government surveillance of their phone conversations than email surveillance, or video surveillance in public restrooms or department-store dressing rooms.

Security Hole Found in Crypto Program GPG
IDG News Service (03/13/06), J. Niccolai

Developers of the open-source GnuPG encryption software say the program has a security flaw that may enable an attacker to sneak malicious code into a signed email message. GnuPG, also known as Gnu Privacy Guard, is an open-source version of the PGP encryption program used for encrypting data and creating digital signatures. The GnuPG team disco-

vered the flaw when they were testing the patch for a previous vulnerability reported last month. "Someone who's able to intercept the message as it's transmitted could inject some data, and then the person who verifies the signature would be told it's a valid, unaltered message," says Secunia CTO Thomas Kristensen. "That's one of the main purposes of the program, so it's quite significant." Secunia ranked the flaw as "moderately critical." It affects all versions of GnuPG prior to 1.4.2.2, and users are being warned to upgrade their systems immediately to that release.

VM Rootkits: The Next Big Threat?
eWeek (03/10/06), R. Naraine

Researchers at Microsoft Research and the University of Michigan have partnered to develop prototypes for virtual machine-based rootkits that significantly push the envelope for concealing malware and that can maintain control of a target operating system. The proof-of-concept rootkit, called SubVirt, exploits known security flaws and drops a virtual machine monitor (VMM) below a Windows or Linux installation. The rootkit is impossible to detect once it is put into a virtual machine because it can not be seen by security software running in the target system. The prototype will be presented at the IEEE Symposium on Security and Privacy later this year. It was created by Microsoft's Cybersecurity and Systems Management Research Group, the Redmond, Wash., unit responsible for the Strider GhostBuster anti-rootkit scanner and the Strider HoneyMonkey exploit detection patrol. "We used our proof-of concept [rootkits] to subvert Windows XP and Linux target systems and implemented four example malicious services," the researchers stated in a paper describing the attack scenario. "[We] assume the perspective of the attacker, who is trying to run malicious software and avoid detection. By assuming this perspective, we hope to help defenders understand and defend against the threat posed by a new class of rootkits," says the paper. The SubVirt project implemented VM-based rootkits on two platforms and was able to write malicious service without being noticed, according to the group.

IETF Taking on 911 Problem Within VoIP
Network World (03/13/06) P. 32; C.D. Marsan

The IETF is working on a technical solution that could solve the problems of how to best route emergency communications such as 911 calls over the Internet and how to ensure that police and firefighters can locate and respond to VoIP 911 calls made from office buildings. The solution, which is called Emergency Context Resolution with Internet Technologies (ECRIT), will allow an IP phone to obtain its location information - such as a street address or office number - when it is used to dial 911. The IP phone will then query a database using a new mapping protocol that will take its location information and find the appropriate emergency call centre. After the emergency call centre is found, the IP phone will place a call to that emergency call centre, which will be given the location of the caller. ECRIT will require enterprises to make a number of changes, including upgrades to their IP phones and IP PBXs. Companies will also need to create a database with the location of every IP address on the network. J. Peterson, a NeuStar fellow and a member of the IETF leadership who is advising the ECRIT working group, says enterprises may end up using DHCP to acquire the physical location of IP addresses. "It's very simple to provide DHCP mapping to push location information down to the phone", Peterson says. ECRIT systems will not likely be deployed for several years, IETF leaders say. "This is not something that is going to get changed overnight". Peterson says.