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

Δελτίο 31
1 Ιουλίου 2006

Auditor's Report Criticizes Florida's Voter Database
Computerworld (06/26/06) Songini, Marc

Florida Auditor General W. Monroe announced in a report published earlier in June that the state's voter registration information can be at risk for theft, corruption, access that is not authorized, and change, in spite of the most stringent effort of elections authorities. The report discovered multiple IT security problems with Florida's main voter registration database. For example, says Florida auditor general's office IT audit manager John Ingram, the system review determined that a state employee was inappropriately granted access to the database and that a worker whose contract was concluded mistakenly held on to access. The auditor's report suggests that Florida Secretary of State S. Cobb's office establish a set of security protocols to help county authorities make certain that Florida Voter Registration System information is shielded from unapproved access. In addition, the report calls on Florida to set up virus protection, patch management, upkeep, and system recovery standards. Consultant P. Hawthorn points out that possible security and information-integrity troubles with voter registration databases are not new to Florida.

Some Rights Reserved: Advancing Flexible Copies
New York Times (06/26/06) P. B1; Rohter, Larry

A worldwide alliance of artists, scientists, and attorneys met in Rio de Janeiro this past weekend to establish a "creative commons" that permits artists and others to determine which rights to their work they want to keep and which they would prefer to share. The Creative Commons system permits creators and patrons of culture to see or listen to a digital work and to copy, remix, or try it out, so long as the author is correctly credited. Since the launch of the Creative Commons idea three years ago, around 145 million "creations" have been registered, and over 100 million of those licenses have been given out in the past six months. Blogs comprised the biggest number, followed by images, and then music, although the video industry is expanding. Microsoft last week made available a plug-in for Windows Office software that allows users to label their own creations, such as Word documents and PowerPoint presentations, with a Creative Commons license. Activists from several nations, however, including Australia and France, contend that musical collection societies are attempting to stop artists from making their work accessible under any system other than typical copyright. These groups, which obtain performance royalties on music from radio stations, recording firms, and others, have threatened to fine or bring action against musicians who license their work via Creative Commons.

Modern Relics
Government Computer News (06/19/06) Vol. 25, No. 16,Jackson, William

The National Institute of Standards and Technology (NIST) recently hosted a workshop addressing the problem of data loss, attempting to craft a strategy for government, industry, and academia to identify what information should be preserved, and how they should be preserving it. Conference participants estimate that every 15 minutes the world produces enough

digital information to fill the Library of Congress, and, though much of it is important to no one, in some areas the creation of meaningful data is outpacing the expansion of digital storage capacities. "So much information is digital, and people are feeling the pain of losing access to their information," said NIST's J. Lubell. The conference participants agreed on the need to develop interoperability standards for data storage across software and hardware platforms. The National Archives and Records Administration and the Library of Congress are working to preserve digital materials in compatible formats. The library is working with other government agencies and outside contractors to develop a national strategy for the collection and preservation of the fast-growing body of digital material. NIST is especially concerned with the preservation of engineering data, which have become too complex for humans to process without the aid of machines. CAD applications deal with levels of mathematics beyond human comprehension, which binds the designs to the software. When the software becomes obsolete, the designs are at risk of getting lost unless they were created with an eye for interoperability. The private sector has not devoted enough attention to the problem because it is not seen as an immediate business concern, says Lubell. "The business case has to be made first" if people are expected to use standards, he says.

Analysis Finds e-Voting Machines Vulnerable
USA Today (06/27/06) P. 14A; A. Stone

The majority of the electronic voting machines that states have been purchasing since the 2000 presidential election "pose a real danger to the integrity of national, state, and local elections," according to a report issued by the Brennan Center for Justice. The report cites more than 120 vulnerabilities in the three most popular systems: touch-screen machines and optical-scan systems with and without paper trails, which together account for 80 percent of the machines that will be used in the upcoming November elections. Though there has yet to be a reported case of voting machines being hacked in an actual election, the Brennan Center's Lawrence Norden notes incidents of similar software attacks on computerized slot machines. "It is unrealistic to think this isn't something to worry about," he said. The report comes amid primary season as concerns about the security of e-voting machines have been mounting. At least six states have seen lawsuits filed attempting to block the purchase or use of electronic systems. The report does not target specific machines, but rather argues more broadly that the e-voting systems in use today are inherently problematic. It finds that the easiest form of attack would be to switch votes from one candidate to another using corrupt software, and that machines that use wireless components are the most vulnerable. Without regular audits, machines with paper trails are just as vulnerable as those without, the report finds. It concludes that states should ban wireless components (a measure so far implemented only by California, New York, and Minnesota) and routinely conduct audits to compare voter-verified paper trails with electronic records.

US Cybersecurity Chief Abruptly Resigns
Associated Press (06/28/06)

Giving just one day of notice, the U.S. government's cybersecurity chief resigned from the Department of Homeland Security after holding the post for one year. A. Yoran's resignation comes amid strident calls from technology leaders and some lawmakers to broaden the range of his authority and give him more money for protection initiatives. Yoran had previously shared with colleagues his frustration over the perceived lack of attention that the department paid to cybersecurity. It is unclear who will step in for Yoran even on an interim basis. Yoran said that he "felt the timing was right to pursue other opportunities." A department spokes-

woman praised Yoran for his contributions and said that cybersecurity remains a high priority, and that the department will work quickly to find a replacement. Industry leaders were unhappy that as a director, Yoran, who led a division with 60 employees and an $80 million budget, was at least three bureaucratic levels removed from the Homeland Security Secretary, and had unsuccessfully lobbied to elevate Yoran's position to the level of assistant secretary. A bill to that end has stalled in Congress. Department officials argue that cybersecurity issues should command as much attention as threats to physical structures, and that they should be addressed in a coordinated fashion because the vulnerabilities to each often have a common source. Under Yoran's tenure, the department implemented a cyber-alert system to notify subscribers about significant Internet attacks as they arise, along with directions to help users protect themselves. The department also created a blueprint of the government's nexus of interconnected electronic devices so that they could be routinely scanned for weaknesses that intruders could exploit.

Securing America's Power Grid
Iowa State University News Service (06/26/06)

Researchers at Iowa State University believe a network of wireless sensors could be used to monitor America's power lines for suspicious activity. A. Somani and J. Junkins are leading a team of computer and engineering experts who are developing a monitoring system that makes use of a network of wireless sensors mounted with a tiny camera to watch movements along power lines. The monitoring system could improve national security, and also be used to watch for conductor failures, tower collapses, hot spots, and extreme conditions. "Power companies would have additional abilities to view their systems and that would assist in disaster recovery," Somani says. The team continues to make progress on a prototype system, and recently showed off their work at Iowa State's Wireless and Sensor Networking Laboratory. They are now in talks with power companies to test the monitoring system on the electrical grid. The project includes designing a diagnosis algorithm to determine fault conditions and predict faults, and a decision algorithm to reconfigure power networks to prevent cascading blackouts. The researchers received a $400,000 grant from the National Science Foundation and a $150,000 grant from Iowa State's Information Infrastructure Institute for the project.

Net Defenses May Be in Danger
Dallas Morning News (06/22/06), C. Harrison

The simple test that asks a user to type in a series of squiggly letters or numbers when making a purchase or conducting some other sensitive application on the Internet, long a stalwart of Web-based security, is "getting to the point where it's almost defeated," according to Luis von Ahn, a post-doctoral fellow at Carnegie Mellon University's computer science department. "The ones not yet defeated by computers are really hard to read for humans. But they'll be defeated pretty soon." Computers now have the sophisticated programming required to read all but the messiest distorted-letter tests, sending computer scientists in search of a replacement. The tests are failing because computer scientists are working to improve the text-recognition ability of computers for benign applications, though once the technology exists, hackers will not be far behind. The current tests, known as Captchas, a term coined by Carnegie Mellon researchers for "Completely Automated Public Turing test to tell Computers and Humans Apart," date back to the late 1990s. Some Captchas display letters that are only slightly distorted, but are crisscrossed with lines overlain on a grainy background, while others make the letters float and swirl. To beat the text-based Captchas, some hackers have

reportedly paid users to enter the correct information, while others have been able to detect patterns in the characters or the code used to create them. Still others have developed computers that are advanced enough to actually read the symbols in the same way that supercomputers have been able to defeat chess masters. Image-based Captchas, where a series of otherwise unrelated pictures might have one common element, can be harder to crack, and Google's Blogger service has begun offering an audio Captcha for sight-impaired users.

US Unprepared for Net Meltdown, Blue Chips Warn
CNet (06/23/06), A. Broache

The US government is ill-prepared to coordinate an effective recovery response to a major Internet shutdown caused by natural or manmade disruptions, according to a new Business Roundtable report. "A massive cyberdisruption could have a cascading, long-term impact, without adequate coordination between government and the private sector," said Cyber Security Industry Alliance executive director P. Kurtz. "The stakes are too high for continued government inaction." Given the devastating effects many sectors of the economy would feel in the event of a massive Internet outage, the government should be better prepared, the Business Roundtable concluded. "There is no national policy on why, when and how the government would intervene to reconstitute portions of the Internet or to respond to a threat or attack," the report noted. The US Computer Emergency Readiness Team is primarily responsible for coordinating cyberattack responses. The report recommends that the government establish a means for providing global-scale advance warnings of Internet disruptions, and release a policy that specifically assigns roles to business and government representatives should such an emergency occur. Other recommendations include the setup of formal cyber-disaster response training programs, and the allocation of more funding for cybersecurity protection.

Cyberprotection Takes Center Stage
Washington Technology (06/26/06) Vol. 21, No. 12, P. 48; A. Lipowicz

The National Infrastructure Protection Plan should address the vulnerabilities of the nation's virtual assets, such as the networks that relay data between major power plants, as well as physical assets, leaders from the computing industry argue. Meeting under the auspices of the IT Sector Coordinating Council, IT executives and cybersecurity experts are developing recommendations that they hope to discuss with the Homeland Security Department's National Cyber Security Division to develop a protection plan for critical IT infrastructure. IT is one of the 17 economic sectors expected to complete its preparedness plans, with the others including sectors such as energy, food, water, and telecommunications. Traditional infrastructure defense plans have focused on physical structures, but assets in cyberspace are different, and one of the critical challenges is evaluating how well the Internet could withstand a major attack on a national scale. There are also the questions of which assets overlap with telecommunications, and who should shoulder the cost of protecting resources that could have multiple classifications. "We're defining [IT critical assets] by critical functionality," said P. Kurtz of the Cyber Security Industry Alliance. "We're asking: What is the top-level functionality that needs to be there? What needs to be there reliably 99.9% of the time?" Ultimately, the list of critical assets will likely include some physical resources on it, such as servers, routers, and the Internet exchange sites MAE-East and MAE-West, though those sites could also be included in the telecom list. Physical assets are less important today than they were five years ago, because operators have widely disseminated them throughout the country to

minimize the disruptive impact of a localized attack. The ongoing convergence of IT and telecom may eventually eliminate the need to divide assets between the two industries.