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

Δελτίο 17
30 Μάρτη 2006

Voter Group Sues to Ban Touch-Screen System
San Francisco Chronicle (03/22/06) p. B2, J. Wildermuth

The voting rights group Voter Action has filed a suit to revoke California's conditional certification of Diebold's touch-screen voting system, citing vulnerabilities the group claims hackers could exploit to manipulate election results. "We can't have trustworthy elections with Diebold's voting machines," said L. Finley, co-director of Voter Action. "They are insecure and easily hacked." Diebold insists that its machines are reliable, despite the flaws reported in a study earlier this year that echoed the findings of Finnish computer expert Harri Hursti. By using the memory cards, a hacker could change the election results without even a password or any special access to the machines. After the 2002 Help America Vote Act, many of California's 52 counties began shopping for new systems, and while the suit will not affect the June 6 primary election, it casts a shadow over the counties that are preparing to use the Diebold machines for the November election. While he admitted that the suit puts the counties in a difficult position, Finley blames Secretary of State B. McPherson for certifying an unreliable system.

DNS Servers Do Hackers' Dirty Work
CNet (03/24/06), J. Evers

Hackers have begun using DNS servers to magnify the scope of Internet attacks and disrupt online commerce in a variation on the traditional distributed denial-of-service (DDOS) attack. VeriSign sustained attacks of a larger scale than it had ever seen last year. Rather than the typical bot attack, VeriSign was being targeted by domain name system servers. "DNS is now a major vector for DDOS," said security researcher D. Kaminsky. "The bar has been lowered. People with fewer resources can now launch potentially crippling attacks." DNS-based DDOS attacks follow the familiar pattern of inundating a system with traffic in an effort to bring it to a halt, though the hackers responsible for the attacks are more likely to be professional criminals looking to extort money than teenagers simply pulling off a prank. In a DNS-based DDOS attack, the user would likely dispatch a botnet to flood open DNS servers with spoofed queries. DNS servers appeal to hackers because they conceal their systems, but also because relaying an attack via a DNS server amplifies the effect by as much as 73 times. DNS inventor P. Mockapetris likens the DNS reflector and amplification attack to clogging up someone's mailbox. Writing and mailing letters to that person would be traceable and time-consuming, while filling out the person's address on numerous response request cards from magazines will cause large quantities of mail to pile up quickly without divulging the responsible party's identity. In a bot-delivered attack, users can block traffic by identifying the attacking machines, though blocking a DNS server could disrupt the online activities of large numbers of users. The DNS servers that permit queries from anyone on the Internet, known as recursive name servers, are at the core of the problem. Mockapetris called the operators of these open servers the "Typhoid Marys of the Internet", and said "they need to clean up their act".

A Quantum Leap for Cryptography
Government Computer News (03/20/06), Vol. 25, No. 6, W. Jackson

In a significant advance in quantum cryptography, a team of international researchers has developed a photon detector capable of creating and exchanging cryptographic keys at 100 Mbps, a peak speed 20 times faster than previous technologies. Built mainly from off-the-shelf pieces, the equipment runs on DARPA's Quantum Key Distribution test bed system. Because reading a photon changes its state, quantum keys created by photons are undetectable to eavesdroppers. Accelerating the process of creating keys is critical to the swift deployment of one-time pads, the lists of random cryptography keys transmitted among senders and receivers that are considered to be the most secure form of cryptography. As computing power continues to advance, quantum cryptography will enjoy a growing number of applications, such as securing a video stream with the rapid production and resetting of keys. Quantum cryptography will cross the threshold of justifiable expense once the cost of deployment is eclipsed by the value of transmitting information with added security, said C. Williams of the National Institute of Standards and Technology. MagiQ already offers a quantum cryptography package, though CEO R. Gelfond admits that it is not yet ready for widespread deployment. The new detector is based on a modified radio astronomy receiver that is a major departure from existing technologies. "This is a fundamentally new type of detector", said BBN Technologies' J. Habif. "The old one is solid state circuitry. This is superconducting technology". A closed-cycle refrigerator lowers the detector's temperatures down to 3 degrees Kelvin, though Habif admits that it is not very efficient. Connecting to DARPA's network that links BBN, Harvard University and Boston University, the system operates at a sustained rate of 100 million pulses per second.

Unsafe at Any Airspeed?
IEEE Spectrum (03/06) Vol. 43, No. 3, p. 44, B. Strauss, M. Morgan, J. Apt

Studies by NASA and Carnegie Mellon University researchers imply that portable electronic devices (PED) carried onto aircraft by consumers emit radiation that can potentially interfere with critical aircraft instruments while in use. The Carnegie Mellon researchers monitored the radio frequency (RF) environment on 37 passenger flights in the eastern US between September and November 2003, and successfully identified emissions from cell phones as well as other consumer devices. The study led to the conclusion that there is a regular occurrence of cell phone calls made from commercial aircraft, in clear violation of FCC and FAA regulations, and also suggested that at least one passenger does not turn off his or her cell phone on most flights. The researchers found not only a profound lack of awareness among passengers of the reasons behind current PED policies, but disbelief that the use of such devices on flights constitutes a major safety risk. The Carnegie Mellon and NASA studies indicate a clear and present danger that cell phones can make GPS instrumentation useless for landings, and support the theory that cell phone emissions may have contributed to accidents. Beyond an outright ban on PED use in aircraft cabins, which is unlikely, the authors recommend that airlines, regulators, and aircraft and equipment makers must practice risk analysis and nurture the development of adaptive management and control via five strategies. There must be a joint industry-government initiative for assessing, testing, and promoting improved communications between aviation professionals and the public; NASA's Aviation Safety Reporting System must be enhanced to once again support statistically meaningful time-series event analyses; in-flight RF spectrum measurements should continue; real-time RF emission monitoring by flight crews must be facilitated; and the FCC and the FAA must collaborate on harmonized electronic device emission and vulnerability standards for avionics.

Primary Voting-Machine Troubles Raise Concerns for General Election
USA Today (03/28/06) P. 1A; J. Drinkard

Voting-machine difficulties in Texas and Illinois have revived concerns that this year's election will be fraught with glitches. Since the Help America Vote Act required states to modernize their voting equipment, it is estimated that in this year's election more than 30 million voters will be using unfamiliar machines. Concerns about the reliability and security of new e-voting systems have reverberated throughout the country, and early problems in primary elections have already materialized in two Illinois jurisdictions - Chicago and Cook County - where precinct judges were untrained, and paper jams and misplaced equipment caused long delays in tallying the ballots. In Texas, state Supreme Court candidate S. Smith is contesting the March 7 primary due to count irregularities. An initial ballot tally in Fort Worth had 150,000 votes recorded, though there are only one-third that number of voters. State spokesman S. Haywood says the irregularities were the result of human error, and the problems have been fixed. In May, 10 states will hold primaries, including Pennsylvania, which is "a disaster waiting to happen," according to John Gideon, director of VotersUnite.org. The new systems will be up to the task, however, retorts M. Shafer of Sequoia Voting Systems, which provides voting machines to Pennsylvania and 19 other states. ACM's US Public Policy Committee recently issued an in-depth report on the accuracy, privacy, usability, security, and reliability issues of statewide databases of registered voters.

Professor to Try to Hack Voting Machines
Pittsburgh Post-Gazette (03/27/06), J. Sherman

After promising to pay $10,000 to anyone who can hack into a touch-screen voting machine without being detected, Carnegie Mellon computer science professor M. Shamos is going to try himself. With thousands of computer scientists having raised doubts about the security of voting machines, Shamos will travel to Harrisburg to test the Sequoia AVC Advantage machine that Allegheny County intends to purchase. He has conducted more than 100 tests on voting machines in five states, and feels that he is better qualified than most to assess the vulnerability of e-voting machines. To meet the requirements for federal aid under the Help America Vote Act, Pennsylvania must have updated equipment in all of its counties. "If the system meets the requirements of Pennsylvania law, I'll recommend it," Shamos said. "If it doesn't, I'll have no hesitation in recommending against certification, even though it would throw elections in this county into a tizzy." Shamos has been certifying voting machines in Pennsylvania since 1980, and had been ready to quit the business when the 2000 election fiasco occurred, prompting a new level of concern about voting machine reliability. Shamos has tested the Advantage machine before, and this time he will spend up to nine hours searching for flaws in the machine's security, reliability, or usability. Voting rights advocates in Allegheny County have raised similar concerns as the Verified Voting Foundation, the California-based organization that has led the call for equipping machines with a mechanism to produce a paper trail for voters to confirm the accuracy of their ballot. D. Dill, the organization's founder and a former student of Shamos', favors optical scan devices, but Shamos says those systems can fall prey to human error as well, and that no evidence of fraud has yet to appear. Shamos has never approved the addition of a paper trail to any system.

Council to Draw Up Cyberattack Response
Washington Technology (03/27/06) Lipowicz, Alice

The IT Sector Coordinating Council is in talks to set up a national IT disaster response system as it prepares to draft a sector-specific plan for protecting the nation's computer networks

against a terrorist attack or other disasters, says G. Copeland, the group's chairman and Computer Sciences vice president. The council is asking for ideas from the IT industry and the Homeland Security Department as it starts work on the sector-specific critical infrastructure protection plan at its April 4 meeting, Copeland says. The council expects the plan to be complete by September. One of the main goals during the drafting of the plan is to involve government officials very early on in the process since IT companies have complained in the past that they have not been asked for their input on infrastructure protection by federal agencies until the last minute, says Copeland. Some issues affecting the IT council include if and how IT companies should share sensitive data about their cyber vulnerabilities with the government, how that information will be protected and used, protocols for sharing information with other sectors, and how to assess the vulnerability of IT assets. The council consists of 33 members and was organized back in November 2005 as one of 17 sector councils representing water, energy, financial services, food. and other areas.