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

Δελτίο 71
26 Απρίλη 2007

Audit Finds Many Faults in Cleveland's '06 Voting
New York Times (04/20/07) P. A20; B. Driehaus

Following a 5 month audit, Ohio's newly elected secretary of state J. Brunner ousted Cuyahoga Country's entire four-member Board of Elections for numerous problems at polling places during the 2004 election. Cuyahoga County, which includes Cleveland, experienced problems that included lines at polls several hours long, poorly trained and absent poll workers, polling places that opened late, and problems with electronic voting machines. The audit found that some batches of ballots registered in optical scan machines were scanned twice, producing a double count of those ballots, and other ballots were deleted because of flawed data and were never rescanned due to human error. The county used machines from Diebold Election Systems and Microsoft's JET file-sharing database system, which was known to have problems that could result in database corruption. Microsoft's S. Massey said any database is subject to corruption if a connection is lost while a transfer is in process. Massey confirmed the committee's finding that Microsoft recommended that a operation as large as Cuyahoga County's should use a different system. Former ACM President B. Simons said, "There is no excuse for Diebold's having used such an insecure and unreliable database. There were far more reliable databases available over 20 years ago." The audit committee has recommended extensive changes, including eliminating either optical scanners or touch-screen machines, to ensure future elections are less troublesome.

Lawmakers Call for E-Voting Paper Trails
IDG News Service (04/18/07), G. Gross

US lawmakers are pushing to have paper printouts incorporated into electronic voting systems to ensure there is a paper record of voting results. In a highly contested congressional election in Florida, more than 18,000 voters failed to cast ballots on e-voting machines, and the Republican candidate won by fewer than 400 votes. G. Hillman, a member of the US Election Assistance Commission, warned Congress not to rush paper-trail requirements, as at least 180,000 direct recording electronic machines across the country would have to be upgraded or replaced. Hillman said introducing new equipment while trying to recruit and train poll workers for a presidential election, which is only a year and a half away, creates the possibility of colossal confusion. Missouri Secretary of State R. Carnahan called on Congress to create flexible time frames for any changes in e-voting requirements, telling Congress not to create expectations that are unobtainable for local election officials. R. Hite, director of information technology architecture and systems for the US Government Accountability Office, said several groups have voiced concerns about the security and reliability of electronic voting systems, and called on federal, state, and local authorities to focus their attention on correcting the very legitimate problems. An extensive GAO review found that many jurisdictions did not use the most current voting system standards, and many do not consistently monitor election performance.

The Memory Hacker

Popular Science (04/07) Vol. 270, No. 4, P. 66; S. Handelman

Memory restoration and a cure for cognitive dysfunction could be the key benefits of an implantable device designed to re-create thought, which University of Southern California neuroscientist T. Berger has been developing for the past decade. The project is in an early phase, but has reached an important milestone with the creation of a chip that is able to converse with live rat brain cells; Berger believes his concept is viable because cognitive dysfunction is, in his words, "essentially a signal-processing problem." Among the agencies underwriting Berger's project are the National Science Foundation, the National Institutes of Health, the Pentagon's Office of Naval Research, and the Defense Advanced Research Projects Agency. Making the chip bidirectional--a sender as well as a receiver--is the major challenge Berger's team faces. The effort dovetails with Berger's long-term goal to reduce higher brain functions to a simple set of mathematical equations. The memory chip is designed to redirect sensory input--sound, sight, taste, etc.--around damaged hippocampal tissue by mathematically mimicking the functions of the injured neurons; the input signals would be intercepted, digitized, and processed by the chip, which would then convert them back to analog signals and reroute them back into the hippocampus. Among the technical challenges is devising a technique for reducing the heat output of the implant's transistors to prevent damage to healthy brain cells. Berger's work has courted controversy, with ethicists warning that the memory chip could shatter concepts of identity and alter healthy memories. Director of Dartmouth College's Neukom Institute for Interdisciplinary Computational Scientists R. Granger Jr. is convinced that "replicating memory is going to happen in our lifetimes, and that puts us on the edge of being able to understand how thought arises from tissue--in other words, to understand what consciousness really means."

Tragedy Spurs Renewed Interest in Mining Internet to Spot Killers
Star-Ledger (NJ) (04/23/07), K. Coughlin

In an effort to prevent future tragedies like the one at Virginia Tech, the government is exploring a variety of controversial data-mining projects that search Web sites and documents for subtle patterns and associations that could expose potentially dangerous people, including shooters, terrorists, and sexual predators. R. Srihari, a computer scientist at the State University of New York at Buffalo and an expert on document analysis, believes these automated systems could catch potential criminals by scanning blogs, audio, and video files on Web sites such as MySpace, Facebook, and YouTube for clues of potential trouble. "It's not inconceivable to try and do that," Srihari said. "Are we there yet? Probably no. But does the technology exist and is it feasible? Yes. And I think we have to, for the safety of people." Privacy advocates are concerned the government could compile dossiers on millions of Americans using these data-mining operations. "The cost to law-abiding citizens is way too high given the remote possibility of benefits," said Jim Harper of the libertarian think tank the Cato Institute. According to the Government Accountability Office, by 2004, some 52 agencies had data-mining projects, or were planning to do so, with the Department of Homeland Security running nine programs and planning to create three more.

Gov't Straining to Secure Computer Systems
Washington Post (04/19/07), B. Krebs

Security experts from the Commerce and State departments told the House Homeland Security Committee's cyber-security panel on Thursday that federal computer networks are being targeted on an unprecedented level and that recent high-profile compromises at two federal agencies are visible symptoms of a government-wide security epidemic. J. Dixon, director of the Department of Homeland Security's National Cyber Security Division (NCSD), said federal agencies are fighting and cleaning up after more digital attacks against their information systems then ever before. In 2006, the NCSD received reports on almost 24,000 security "incidents," ranging from attacks probing electronic networks to find vulnerabilities, to computer viruses, to unauthorized access of government information resources. Dixon said the NCSD is already on track to receive more than double that number of incident reports in 2007. "Report cards" issued by a congressional oversight committee last week gave both the Commerce and State departments failing grades, and the Department of Homeland Security, which is responsible for ensuring that federal information systems are protected and is supposed to lead the nation by example, received a grade of "D." "I don't know how [DHS] thinks it's going to lead this nation in security cyberspace when it can't even secure its own networks," Rep. J. Langevin, D-R.I., said. "Not only are these grades embarrassing, they're dangerous."

Open Source, Transparency and Electronic Voting
Linux Insider (04/18/07), J. Mello

Critics of electronic voting systems are calling for any software used in voting systems to be made open source and fully transparent. University College Dublin in Ireland computer science lecturer and open source voting software researcher J. Kiniry said using open source software for electronic voting would add credibility to the process. Kiniry said with open source, "not only can experts evaluate the software and make sure it does what it says it does, but it also increases the level of trust that normal, non-expert users can have in that software system." Software engineer John Washburn pointed out a disturbing trend with electronic voting's reliability and testing systems. "Everyone who is not paid by a vendor who has looked at existing electronic voting machinery has found significant flaws," Washburn said. "Moreover, they've never found the same flaw twice. That tells me that that must be some defect-dense code. Not only do you find something every time someone looks at it, you find something new every time someone looks at it." Speaking before a congressional subcommittee on elections, Electronic Frontier Foundation (EFF) staff attorney M. Zimmerman said the EFF felt hindered, both as election observers and as legal counsel for voters who felt compelled to challenge election results due to malfunctioning equipment, by the lack of transparency in the electronic voting "closed technological regime." Some argue that creating open source voting software will expose electronic voting systems to hackers, but Washburn says that argument is based on the "security through obscurity model," and anyone who takes security seriously knows better.

P2P Worms Get Their Turn
InfoWorld (04/16/07), M. Hines

Experts claim that botnet-driven mass attacks are replacing traditional worms as the platform of choice for a growing array of skilled and well-funded fraudsters. This trend is illustrated by the P2P, or Storm, worm currently evading anti-virus systems and propagating itself through botnet commands. The new breed of P2P worms are delivered through large networks of hijacked computers and have sophisticated techniques, such as exploiting private networks to contact external servers. Employed by a variety of customers for a variety of purposes, botnets are easy to use; single-purpose botnets can be abandoned after use, making pursuit even more difficult. Many of those involved in creating the attacks are from China and Eastern Europe, and criminal groups with pools of laundered money are becoming involved as well. Experts worry that organizations are consolidating to mount large-scale attacks with increasing professionalism, and urge the IT security community to prepare for the growing botnet problem.