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

Δελτίο 61
12 Φλεβάρη 2007

Congressman Renews Push for E-Vote Paper Trails
Computerworld (02/06/07), M. Songini

US Rep. R. Holt (D-N.J.) has introduced his bill requiring a paper trail for electronic votes once again in Congress. A Capitol Hill controlled by Republicans did not act on the Voter Confidence and Increased Accessibility Act last year, but Holt hopes the outcome will be different now that Democrats are in power. "Until we require that voting systems produce a voter-verified paper ballot, the results of our elections will always be uncertain," Holt said in a statement. Under the bill, the auditing process would consist of routine random hand counts of precincts in every Congressional voting district. The proprietary software of e-voting vendors would come under scrutiny in examinations by independent inspectors, and voting officials would have to document their chain of custody during elections as a way to improve the transparency of the security of their hardware. The reintroduction of the bill comes at a time when a lawsuit filed by Christine Jennings, a Democrat in the 13th Congressional District in Florida, is still pending on whether the results of her race, in which there were 18,000 missing votes, will be invalidated and there will be a recount.

Internet Servers Handle Major Global Attacks
Associated Press (02/07/07), T. Bridis

Three of the 13 computers that help process global computer traffic were briefly overwhelmed on Tuesday, but due to increased distribution of workloads to computers around the world, the attacks were not as serious as those that confronted the same servers in 2002. UltraDNS, the organization that handles servers managing traffic for .org sites, was the target of the attack, which some suspect originated in South Korea. NeuStar, which owns UltraDNS, reported only that it had registered an unusual rise in traffic. There was no clear reason for the attacks, other than "maybe to show off or just be disruptive; it doesn't seem to be extortion or anything like that," says the Supercomputing Center in San Diego's D. Wessels. Included in the targeted "root" servers were those run by the Defense Department and ICANN. "I don't think anybody has the full picture," said ICANN chief technical officer John Crain. "We're looking at the data."

UM Study: Hackers Attack Every 39 Seconds
PRNewswire (02/06/07)

A study by University of Maryland researchers from the J. Clark School of Engineering observed the activities of hackers as they try to gain access to a computer and exploit it. "Brute force" hackers were the focus of the study, which set up four Linux computers with weak security and Internet connections. The computers were attacked an average of 2,244 times each day, or every 39 seconds on average, confirming suspicions that the average computer is almost constantly under attack. "Most of these attacks employ automated scripts that indiscriminately seek out thousands of computers at a time, looking for vulnerabilities," says lead researcher M. Culkier, an affiliate of the Clark School's Center for Risk and Reliability and Institute for Systems Research. The study documented the most commonly attempted user names, which were "root" and "admin," and the most attempted passwords, which were identical to, or variations of, the user name, as well as "123." After gaining access, hackers would typically check the computer's software configuration, change the password, check the configuration again, and download and install a program, which they would then run. "Often they set up back doors'--undetected entrances into the computer that they control--so they can create 'botnets,' for profit or disreputable purposes," Culkier says.

Bush Seeks Spending Increases in Research, Surveillance
CNet (02/05/07), A. Broache

President Bush on Monday announced his budget proposal for next year, placing priority on homeland security, the war on terror, and global competitiveness via the American Competitiveness Initiative. Under Bush's proposal the NSF would receive a 6.8 percent increase in funding, with a large portion of that being dedicated to "research and related activities." NSF's budget includes $390 million for nanotechnology research funding, a 4.5 percent increase, and $994 million for the Networking and Information Technology Research and Development program, a 10% increase. However, some programs received less funding, or none at all. For example, funding for the National Institute of Technology's Advanced Technology Program, which explores "unproven, early stage technology," was completely left out of the budget. Homeland Security would get an increase of $21.9 million for its Science and Technology Office of Innovation, but the total funding for the Science and Technology directorate would drop from $848 million last year to $799 in the upcoming year. Bush also announced plans to considerably increase funding for Justice Department programs aimed at intercepting data and investigating international travelers. Bush's budget proposals were criticized by Democrats. House Science and Technology Committee Chairman Rep. B. Gordon (D-Tenn.) praised the funding increases, but said the overall proposal "lacks the priorities and consistency to ensure our competitiveness now and in the long run."

Fighting to Protect Copyright 'Orphans'
CNet (01/31/07), D. Terdiman

A recent US appeals court ruling dealt a blow to Internet activists' effort to stop the extension of copyright protections for out-of-print books and other orphan works by upholding the rejection of a lawsuit filed, among others, by Internet Archive co-founder and director B. Kahle. Nevertheless, the Internet Archive is by no means dead, as Kahle told an audience of listeners at a recent discussion. He explained that the mission of the archive is "to help build the Library of Alexandria version 2, starting with humankind's published works, books, music, video, Web pages, software, and make it available to everyone anywhere at anytime, and forever." The challenge, Kahle noted, lies in constructing a digital domain that permits the creation of and reimbursement for new works and their long-term preservation, while supporting access for the underprivileged as well as different types of access for journalism, scholarship, "and all in the new world." Kahle said resistance to the Internet Archive stems from an earlier copyright battle in which major media companies such as Disney, rather than simply extend terms of copyright for profitable works, lobbied for and got a major restructuring of copyright. This has set up what he called a "legal landmine" of which people are afraid of running afoul. Kahle said there is a clear need for aid in building an open content layer that has no central control, and the potential threat of ISPs violating Net neutrality by choking certain kinds of content is an issue of considerable importance. "I believe we can have long term storage and access--which is key--by building a set of International Libraries in different jurisdictions that have active trade agreements," the Internet Archive director concluded.

Feinstein Will Pursue Paper Record at Polls
San Francisco Chronicle (02/08/07) P. A4; Z. Coile

Sen. D. Feinstein (D-Calif.) later this month will introduce a bill that establishes national standards for e-voting security. "I believe the time has come for Congress to help ensure that we have such a record in all federal elections," said Feinstein, chairwoman of the Senate Rules and Administration Committee. Rep. R. Holt (D-N.J.), who already introduced a similar bill in the House, calls the recent Florida election problems "exhibit A" as to why national e-voting mandates are needed before the upcoming presidential election. His bill requires a paper trail, random manual audits of paper ballots in a small portion of each precinct, and an assurance that e-voting software will be open to regular inspection. Rice University computer science professor D. Wallach has criticized e-voting machine manufacturers for not allowing their software to be tested independently, saying they "shouldn't need to hide behind a veil of secrecy." Opponents of e-voting legislation claim that printers will only add to the problems at the polls, as they are known to jam with varying frequency, and that e-voting machines have proved to be more accurate at vote-counting than other systems. However, Feinstein says current e-voting systems lack the safeguards necessary to prevent fraud. She says, I'm not sure that the most technologically modern machines necessarily yield the best results. I'm from the school that likes to see their mark (on the ballot.)"

Feds Defend Oversight of E-Voting Testing
CNet (02/09/07), A. Broache

The Election Assistance Commission (EAC) held a public meeting on Monday to clear up accusations that it was not being open about its review processes for the independent labs that test e-voting machines. A New York Times article that exposed EAC's ban on Ciber, the largest such testing lab, from conducting any more tests concerned many who felt the commission should be more forthcoming with such information. Questions were also raised as to the reliability of voting systems tested by Ciber for use in past elections. EAC Chairwoman D. Davidson said it is standard practice for labs to "be given a period of time in which they can correct those non-conformities, and that may go on for some time." The National Institute of Standards and Technology has released a good deal of information on the lab review process, such as the complete reports from onsite assessments of the lab, the lab's response, and the names of labs that have applied for the review, according to NIST's D. Alderman. He added that such information is not usually made public because of the tendency for labs to use it to promote themselves or smear other labs. Ciber now has until March 5 to hand in paperwork that EAC will use to decide whether or not to grant the lab "interim" accreditation. Also on this date, the commission plans to stop accepting applications for "interim" status, which has less stringent requirements. A new federal system requires a two-step process for lab accreditation. First, the lab must prove itself in a NIST technical review. If the lab passes this review, the matter is passed along to the EAC, which checks for non-technical concerns such as conflict of interest, organizational structure, and record-keeping protocols.

U.S. Cyber Counterattack: Bomb 'Em One Way or the Other
Network World (02/08/07), E. Messmer

The National Cyber Response Coordination Group (NCRCG) has been formed to draw up a national response should a cyber attack occur that impairs the United States' critical information infrastructure. In such an event, a cyber counterattack or actual bombing of the source of the attack could be carried out, according to the three NCRCG co-chairs from the US-CERT computer readiness team, the Dept. of Justice, and the Dept. of Defense (DoD), although the preferred method would be to warn the source to shut down before being attacked. Given this week's attempted massive denial-of-service attack on the Internet's root DNS servers, "We have to be able to respond," says DoD co-chair to the NCRCG Mark Hall. "We need to be in a coordinated response." Bringing together elements of the private and public sectors for information-gathering efforts is quite a challenge even without considerable disruption to Internet or voice communications. "We're working with key vendors to bring the right talent together for a mitigation strategy," says US-CERT co-chair to the NCRCG J. Dixon. The group plans to speak with 50 other countries that are also monitoring for large-scale cyber attacks. The Air Force has already established a new Cyber Command that would be ready for "network warfare," says Air Force Information Operations Center R&D engineer J. Collins. "Where we had pilots before, we'll have fighters in cyberspace." Any NCRCG recommendations would be subject to approval by the President.

Researchers Invent System to Control and Quarantine Worms Attacking Computer Networks, Penn State Live (02/08/07)

Penn State researchers have developed anti-worm technology that detects and stops worms much faster than conventional systems, and is also able to release any information stopped as the result of a false positive. Rather than using signature or pattern identification, Proactive Worm Containment (PWC) "looks for anomalies in the rate and diversity of connection requests going out of hosts ... [since] a lot of worms need to spread quickly in order to do the most damage," says lead PWC researcher P. Liu. Signature-based systems can take a few minutes to recognize a worm and create a new signature to stop it from spreading, and when these systems decrease the time needed to generate a signature, they can miss worms that are able to automatically mutate. Liu estimates that a worm could only send out a few dozen packets before being quarantined by PWC, compared with the 4,000 packets sent out every second by a worm that recently attacked a Microsoft SQL server. To verify if a suspected host is infected or not, PWC uses vulnerability-window and relaxation analyses that can undo a potential denial-of-service resulting from a false positive. PWC can be seamlessly added to existing signature-based worm filtering systems. Liu admits that his system would not be able to spot slow-spreading worms, but notes that those can already be stopped by current technologies.

Miklau Awarded CAREER Grant to Study Privacy, Accountability
University of Massachusetts Amherst (02/05/07)

University of Massachusetts computer science researcher G. Miklau plans to build a computer database system that improves the management of digital devices' history of past operations and data. The development of the database system will be made possible by a five-year, $500,000 grant from the National Science Foundation's Faculty Early Career (CAREER) grant program. Computer systems preserve the history of their activity as a way to offer some accountability, and this is helpful for detecting breaches, maintaining data quality, and auditing security compliance. "In some settings, however, retaining a history of past data or operations poses a serious threat to privacy," says Miklau. "The fact is, privacy and accountability are both important goals, and system designers need to carefully manage the balance between them." Miklau plans to give the computer database system "memory-less" and accountability-support functions. A prototype database system will be made publicly available.

High Security for $100 Laptop
Wired News (02/07/07), R. Singel

The One Laptop Per Child (OLPC) project has impressed computer experts with the unique design of its machine, the XO, and is now receiving attention for its approach to security. The XO's security lies in the limited permission of each program to access others due to the virtual machines that every program runs in. Although the idea of limiting programs' permission is nearly half a century old, it has placed too much of a security burden on programmers to be instituted, says I. Krstic, head of security for the XO. XO's security system, known as the BitFrost platform, has no security prompt, firewalls, or antivirus software. "Applications can no longer run rampant," says Krstic, as opposed to Windows XP where even Solitaire can access the Web. Only software verified by OLPC or by a participating country can request permissions. The idea is to undermine malware by eliminating hackers' economic incentive. Krstic does acknowledge that interaction between applications will be severely limited, but he says that "99% don't need" to. The XO will also have a system by which it checks in with a country-specific server every day to see if it has been reported stolen; if it has been it completely shuts down, and if not its cryptography-secured "lease" is extended a few more weeks. Krstic sees flaws in every traditional security architecture used in today's computers, including the new Microsoft Internet Explorer's virtual sandbox, which he says, "is trying to impale sandboxing on something that doesn't exist."

For Computer Scientists Exploring Face Recognition, the Question Is 'Who?'
PhysOrg.com (02/07/07), L. Zyga

The human brain is able to recognize a face in 50 ms, and while scientists hope to learn from the way the brain works in order to create computer programs that can do the same, they are eager to find out if computers could perhaps surpass humans in this ability. "It would be a waste not to learn from [the brain], especially since there are no other computer strategies so far that come close to the kind of face recognition performance the human brain exhibits," says Harvard scientist Richard Russell. Humans have the ability to recognize faces in very low-resolution images. Even when given an ideal perfect view of a face, the human visual system "doesn't seem to bother storing perfect models of the objects we see," says MIT's B. Balas, who worked along side Russell on the paper, "Face Recognition by Humans." People seem to use only certain features, such as eyebrows, to identify each other. Faces are processed by adults as holistic images, unlike many other objects. In designing face recognition computers that could be used to find people in a crowd or for the creation of "smart" environments, scientists pay attention to the human visual system's techniques, but remain open to the possibility that a computer could do better. "Too much generalization can be a short-coming," especially when people are in disguise, says MIT's P. Sinha, another contributor to the "Face Recognition" paper. "A detail-oriented scheme, say examining the precise pattern of irises or the exact distances between facial features, might be more appropriate, despite being implausible as human strategies."