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

Δελτίο 67
26 Μάρτη 2007

Florida Officials Warned of E-Voting Glitch Prior to Election
Computerworld (03/20/07), M. Songini

Florida election officials knew of problems in voting machines prior to November's election and failed to take action, according to a memo cited by C. Jennings in the latest stages of her attempt to appeal an election in which 18,000 people who voted in other races did not register a vote. The memo from Election Systems & Software, dated August 15, tells election officials that machines had been "exhibiting slow response times" between the screen being touched and a candidate's name being highlighted, due to a problem with the "smoothing filter" on some models, and that poll workers should be prepared for "slightly delayed" response times for the machines. The smoothing filter is software embedded in the machine's hardware that waits for several consistent reads from the touch screen before highlighting a candidate's name in preparation for casting a vote. Both the voting machine manufacturer and states officials claim that this flaw, which was reported by many on election day, could not have influenced election results. Jennings believes the slow response times could have influenced results. "It's a slap in the face to Florida voters that they [the officials] knew about a problem with our voting machines and did not do everything within their power to fix it," Jennings says. ES&S says a software upgrade was available but had not been certified by the state in time for the election.

A Student-Hacker Rematch and the Second Annual Collegiate Cyber Defense Competition, InformIT (03/16/07), S. Fogie

The annual Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC) is a contest between students tasked with locking down unfamiliar systems and securing their networks, and hackers dedicated to commandeering those networks and pilfering sensitive data. Expectations were high that the hacker team participating in this year's CCDC would have a tougher go of it than last year, as most of the student teams were veterans of last year's competition and would likely be better prepared. Each team was assigned a duplicate system with identical services, service packs, operating systems, and applications, and then left on their own in locking down their assets; all updates and patches had to be downloaded from a separate part of the CCDC network. The students also had to contend with several "unknowns," including a rough access point installed behind the firewall in the 10.10.20.x range and a preinstalled rootkit/keylogger residing on the server. The SANS Institute provided the hacker team, and as anticipated the main intrusion technique was not default passwords and configurations (as it was in last year's CCDC), but the exploitation of a dearth of proper security updates and the use of insecure passwords. The CCDC makes a point to increase students' familiarity with basic incident handling procedures via the incorporation of an Incident Reporting feature into the games and the enlistment of two US Secret Service agents as advisors. The CCDC's chief goal is to offer students the experience of real-world IT business situations, and this is partly fulfilled through the inclusion of Business Injects that mimic the types of requests a typical IT department must regularly contend with. Among the lessons taken away from this year's competition is that an unpatched and unprotected system should not be put online for any reason; reporting procedures require unimpeachable proof that an

intrusion took place; and an IT employee's continued employment hinges on how well he pays attention to customers' needs and performs the tasks he is given.

Internet Research, Uncensored
Chronicle of Higher Education (03/23/07) Vol. 53, No. 29, P. A29; S. Kean

Repressive governments use Web filters to censor scholars' access to Internet content, but these filters can be bypassed by open-source software such as Psiphon and Tor, developed by Western computer scientists. Users of Psiphon, which was designed by the University of Toronto's Citizen Lab, must rely on trusted parties to be on hand in free countries to give them access, while Tor promotes anonymity by routing information through a web of computers so tangled that snoops lose the scent. "You would use Tor if you didn't know anyone," notes sometime security consultant for the University of Toronto D. Vitaliev. "You would use Psiphon if you had someone to trust." Unlike Tor, the Web-based Psiphon does not require any files to be downloaded, which means snoops have no clues to latch on to. Psiphon is very popular with Iranian, Burmese, and Vietnamese diaspora groups, according to Citizen Lab director R. Deibert, who is a member of the Open Net Initiative. The initiative was established to monitor Internet censorship by Harvard University Law School and the Universities of Toronto, Cambridge, and Oxford. Academics in the United States teach Tor in computer security classes, and Psiphon is used to give students a glimpse of oppressive regimes' censorship practices.

Certification on the Ballot
Government Computer News (03/19/07) Vol. 26, No. 6, W. Dizard

NIST and the Election Assistance Commission are developing a reformed version of federal guidelines for voting systems and new standard testing suites for use by accredited testing laboratories. The new guidelines for voting systems would require software-independent technology that would create internal audit trails separate from the paper trail systems that allow voters to verify the accurate recording of their votes. NIST will most likely present the new version of the guidelines this summer, but it will take the EAC until next year to approve them. The public, uniform test suite being developed is intended to "build on the credibility of the labs," explains EAC chair Donetta Donaldson. Before recommending a lab for accreditation, NIST evaluates the lab's procedures for ensuring that voting systems create activity logs and perform other specific functions. Each lab must be re-evaluated every two years. Testing voting systems is different from testing other types of IT due to "the secrecy of the ballot," says C. Coggins of iBeta Quality Assurance, a recently accredited testing lab. "In other types of IT auditing situations, you don't remove the identity of [the person entering data into the system]. But in testing voting systems, you have to pull your audit trail apart." The EAC is also working with states to develop secure processes for removing names from the statewide voter registration databases that were to be completed by January 2006, a deadline that was missed by nearly half of all states. "Now, the public sees not only updates on the voting system guidelines, and additional security built in, but for the first time we have a federal government voting-system certification process," said Donaldson.

Son of TIA Will Mine Asian Data
Wired News (03/22/07), S. Weinberger

Singapore is set to launch a data-mining effort that goes beyond the Pentagon's controversial 2003 Total Information Awareness Program (TIA) proposal, which was scrapped due to an

uproar from privacy groups. The Singaporean program, known as Risk Assessment and Horizon Scanning (RAHS), will search for threats to national security by collecting data across all government agencies, making it the most comprehensive data-snooping program in the world. RAHS creates "a large network that is constantly scanning the horizon looking for weak signals that point toward the possibility of a significant event that would have important implications for Singapore," says the Arlington Institute's J. Peterson, who is consulting for the Singapore project, along with others formerly involved in the TIA program, including D. Snowden and former national security advisor and TIA architect J. Poindexter. Snowden stresses RAHS' ability to spot "weak signals" that would normally be missed by humans. He says, "Instead of having analysts trawl through huge amounts of data to decide what it means, the data is tagged very quickly, then they decide what the patterns in the metadata mean." He also defends the program against privacy advocates, stating that only metadata, not the data itself, would be shared among agencies. RAHS will initially focus on "open source" information until the procedures for working with classified information can be worked out, according to Singapore security official P. Nathan, who adds that the city-state is currently piloting a data anonymization system. Privacy advocates claim that surveillance by a machine rather than humans does not serve to protect individual privacy. Snowden applauds the "pragmatic and forward-thinking" attitude behind RAHS. He says, "Singapore just walked around and saw what they liked, and said, 'The hell with it, let's just make it operational.'"

Tool Turns Unsuspecting Surfers Into Hacking Help
CNet (03/20/07), J. Evans

A new security tool that can make the PCs of unknowing Web surfers search for flaws in Web sites shows that JavaScript can be used for malicious purposes, a fear expressed by many security experts. SPI Dynamics security researcher B. Hoffman developed the tool, known as Jikto, to enhance Web security. "Jikto turns any PC into my little drone," he explains. "Your PC will start attacking Web sites on my behalf, and you're going to give me all the results." The tool, which audits public Web sites by silently crawling through them and sending vulnerability information to a third party, can be embedded in an attacker's site or injected into a trusted site by exploiting a cross-site scripting flaw. Jikto can then connect back to its controller for further instructions. "Half of hacking is collecting information and then sorting it," says Hoffman. "An attacker can now distribute this job to many people." Although Jikto shows that JavaScript can be used maliciously, the traditional vulnerability scanners that hackers use to break into systems are probably more effective. Operating from compromised machines, these vulnerability scanners "can generally scan pretty widely with impunity, or they can just use a chain of proxies," explains Nmap Security Scanner inventor F. Vaskovich. However, since it is JavaScript, Jikto can run in most Web browsers without any way of the user knowing. "As a user you really can't do much against Jikto or other JavaScript-based threats," Hoffman says. "I am not really compromising your computer. That is what makes this so scary." Next, Hoffman plans to work on a version of Jikto that can exploit vulnerabilities and extract data.

Privacy for Domain Owners Moves Forward
Associated Press (03/21/07), A. Jesdanun

Domain name owners may soon have more privacy options when entering contact data in the publicly available Whois database, thanks to a new proposal that was recently endorsed by an important task force. ICANN will hold hearings on the proposal, known as "operational point of contact," during its upcoming meeting in Lisbon, Portugal. Tucows representative R. Ra-

der, a member of the Whois task force, goes so far as to predict that a big change is coming and that domain name owners will no longer have to publicly display their personal contact data on Whois. The database has caused controversy because it stores domain name owners' contact information, including names, email addresses, and phone numbers. This information is publicly accessible and is used by a variety of parties, including law enforcement, ISPs, lawyers, journalists, and spammers. Some domain owners choose to enter fake data, which puts them at risk of losing the domain. But under terms of the new proposal, domain name owners would have a standard option of listing the contact information of third parties -- lawyers, service providers, and the like--instead of their own contact data.