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

Δελτίο 82
11 Ιουλίου 2007

Hackers Hired to Crack California Electronic Voting Machines
KABC-TV (Los Angeles) (07/02/07), N. Miranda

California is conducting a test to see if three types of electronic voting machines approved for use in California elections are vulnerable to hackers. A team of independent hackers from across the country is trying to break into and rig the results on the machines. "The goal is to put to rest any controversy about voting systems or the voting equipment itself," says California Secretary of State D. Bowen. California is the first state to require a full review of voting machines, as well as the first to require the machine vendors to pay for the review. "Our concern is the voter walking up and doing something strange on the machine," University of California Davis computer scientists M. Bishop says. "Another thing we're concerned about is someone, for example, somehow manipulating the machines that count the votes so they count the votes incorrectly." California already requires paper trails and public audits, but the hacking program is another effort to ensure voters that their ballots will be counted. "The goal of this review is for us to do that on voting systems where we can be confident that the effect we have on the presidential primary is the effect that California voters intended," Bowen says. The hackers have until July 20th to break the system.

How Safe Are Wireless Networks?
Dalhousie University (07/04/07), D. Morrison

Wireless security is the focus of research that is being pursued by a team at Dalhousie University. Over the next five years, Dr. S. Sampalli and graduate students from Dalhousie's Faculty of Computer Science will receive $32,000 annually from the National Sciences and Research Council of Canada (NSERC) to study security and resource management in heterogeneous wireless networks. The project will complement another collaborative initiative that seeks to improve the security of wireless networks, which is sponsored by Industry Canada. The researchers hope to learn what makes wireless networks susceptible to exploitation, the different ways the networks can be attacked, and the strengths of applying common security measures. Sampalli also wants to establish guidelines for security best practices for detecting and preventing intrusions. They will study vulnerabilities and prototypes for detecting and preventing intrusions using a test bed. The use of wireless data devices continues to grow, and deployment of the devices could reach 226 million next year. "Unfortunately, the tremendous rapid growth has brought with it a large number of security issues and has exposed numerous vulnerabilities in wireless networks," says Sampalli.

Is Securing Your Network Worth the Money?
Network World (07/03/07), B. Brown

Security researchers discussed IT security at a conference hosted by Carnegie Mellon. Two Dartmouth College Center for Digital Strategies researchers studied the involuntary disclosure of data through peer-to-peer sharing networks at a group of major financial institutions, and determined that lazy or badly organized end users are often responsible for the leakage of sensitive information, while P2P networks are aggressively searched by criminals seeking data to exploit. The researchers recommended the introduction of "file naming conventions and policies to reduce the metadata footprint of their documents." Researchers from Tel Aviv University and the Michigan State University Dept. of Economics presented a paper detailing the interdependent relationship between software vendors' "profit-maximizing behavior" and vulnerability disclosure policy, while USC researchers discussed a technique for quantifying security threats so that organizations can ascertain how much they must budget for commercially available security products to fulfill their security requirements. UC Berkeley, University of Michigan, and HEC Montreal researchers presented a paper focusing on the advantages to vendors of strengthening their software's security and reliability, noting that usually users fail to perceive any difference between a failure's occurrence due to a security or reliability problem and typically consider software bugs to be the source of both kinds of failures. A multi-divisional enterprise's implementation of security countermeasures in the context of variegated information systems controlled by its divisions and in response to various types of damage that the enterprise's information systems and assets can suffer from threats was an issue probed by three Carnegie Mellon researchers. They reached the conclusion that "there are strategic issues in information security decision making and that the distortion due to incomplete knowledge of information systems by the CIO has to be weighed against incentive problems when division managers make decisions."

Lawmakers to DHS: Spend More on Cybersecurity
Federal Computer Week (07/03/07), J. Miller

The House Homeland Security Committee wants the Dept. of Homeland Security's Science and Technology Directorate to allocate more funding toward cybersecurity research and development efforts. The directorate currently has $37 million allocated toward cybersecurity R&D through the year 2011. During a June 27 hearing, committee members peppered the directorate's undersecretary, J. Cohen, with pointed questions about the funding efforts, stating that current funding levels are insufficient. Cohen explained that the DHS assistant secretary of cybersecurity, G. Garcia, has mandated that just 1% of the directorate's funds be allocated toward cybersecurity research. During the hearing, Cohen acknowledged that 1% is too low of a figure, explaining that he would welcome more input from Garcia and DHS CIO S. Charbo on the types of solutions they need. Rep. M. McCaul (R-Texas) says he intends to create a bill forcing the DHS to assess the nation's cybersecurity vulnerabilities. Cohen replied that he supports such a mandate, so long as it also applies to all other federal agencies. Cohen urged entrepreneurs and inventors to approach the DHS "with opportunities to solve problems."

US Government Prepares for Cyber War Games
Ars Technica (07/05/07), J. Reimer

The colossal distributed denial-of-service attack (DDoS) on Estonia's Web sites in May 2007 prompted the United States to both assist Estonia in the aftermath and to review America's own level of readiness for such an attack. Currently, to help scrutinize attack-generated data, the United States is sending an investigative team to Estonia. The team will also train Estonian IT professions in safeguarding their network infrastructure. Meanwhile, the US government established the "Cyber Command," a group that will plan the country's response to similar cyberattacks. In addition, a federal exercise developed to test pandemic preparedness has been revised to incorporate a cyberterrorism response simulation. Because critical services--such as routing infrastructure and DNS--in Estonia were unscathed by the attacks, the significance of the assault seems to lie in the response roused in other nations. Whether or not the Russian government was involved in the DDoS attack, the Estonia incident may be deemed the first international "cyberwar," and as such may raise awareness of modern society's vulnerabilities. The attacks did, however, illustrate the usefulness of international teamwork, for NATO member nations offered assistance and security professionals responded in real time from all over the world. President G. Bush recently thanked Estonia's president for disclosing data about the attacks that could help other countries protect their infrastructures from comparable assaults.

ISU Experts Weigh in on Identity Theft Through New Wireless Technologies
Iowa State University News Service (07/03/07)

Cell phones, BlackBerrys, and other new wireless technologies are being exploited by identity thieves and extortionists, and Iowa State University faculty and staff experts offer commentary on this growing problem. ISU electrical and computer engineering professor D. Jacobson reports that identity theft is becoming more common as criminals learn how to reap profits from data collected from the Internet, and he comments that these persons "are targeting people directly through social engineering using email messages that lure us into providing information that can be used to steal an identity." In addition, criminals are attempting the direct theft of information from computers through the use of rogue programs, and Jacobson recommends that people should be vigilant of what information they disclose to others online, and what programs they download. Meanwhile, ISU associate CIO M. Hope believes victims of identity theft should consult the Federal Trade Commission's National Resource on Identity Theft Web site or a site hosted by Visa; he can offer suggestions for preventing identity theft and warns of a new phishing scam that lures victims with a "greeting card emailed by a family member or friend." Accenture Faculty Fellow in Management Information Systems A. Townsend, who co-authored the book "Information Technology and the World of Work," notes that the growing use of technology that records communication, such as wireless products, generates the potential for messages getting intercepted. His advice is to "be cautious about all conversations over telephones, be doubly cautious about email and instant messaging, and use encryption for private correspondence."

Warning of Data Ticking Time Bomb
BBC News (07/03/07)

The obsolescence of old digital file formats could mean a major loss of knowledge for society, warned UK National Archives CEO N. Ceeney at an event to mark the launch of an alliance between her organization and Microsoft designed to ensure that legacy formats remain accessible. The National Archives preserves nine centuries' worth of written material and over 580 TB of data in older file formats that are no longer commercially available. Ceeney lamented that some digital documents have disappeared for all time because the programs that could read them are no longer extant. "We have worked very hard to embrace open standards, specifically in the area of file formats," stated Microsoft UK director G. Frazer, who said a "digital dark age" is on the horizon unless an effort is made to maintain the readability of legacy formats. Microsoft devised the Open XML document file format, which is used to preserve files from programs such as Excel, Word and Powerpoint, with this goal in mind. Frazer described Open XML as an independently controlled open international standard, but some critics wonder at Microsoft's decision to design its own standard instead of embracing the competing Open Document Format system. Open Rights Group director B. Laurie claimed the move is an attempt at vendor lock-in. The National Archives will be able to access older file formats in the format in which they were originally recorded by running mimicked versions of the older Windows operating system on present-day PCs via virtualization.