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

Δελτίο 119
5 Ιουνίου 2008

Web Vote Offered to Military Abroad
Miami Herald (05/26/08), G. Fineout

Florida's Okaloosa County plans to use the Internet to make it easier for US soldiers stationed overseas to vote. Okaloosa elections supervisor P. Hollarn's plan would allow those living on or near three military bases in the United Kingdom, Germany, and Japan to cast ballots online in the November election. During a 10-day period before Election Day, overseas voters will use a computer kiosk to vote on an encrypted electronic ballot, which will be sent to Florida via the Internet and counted. Poll workers on site will verify that the voter is registered in Okaloosa County. Hollarn says her "distance balloting project" is just like other absentee ballots, except it uses the Internet instead of the mail. However, critics and voting activists say the project is unsafe and goes against a new law that requires the state to use paper ballots. Although voting-rights activists agree that absentee ballots for voters living overseas have been plagued by significant problems, they say the idea of using the Internet to transmit ballots is problematic due to security concerns. Hollarn says the voting mechanism will be safe, emphasizing that the machines and software being used will be reviewed by an independent team of computer analysts.

Managing Computer Fraud
EurekAlert (05/23/08)

Information security researchers are starting to look at computer fraud from a social angle. Southern Utah University computer scientist S. Kesar writes in the International Journal of Business Information Systems that companies should educate management on the impact of organizational structure on security measures, and then let other employees know that management is well informed on security issues. Computer fraud often occurs in organizations that do not facilitate widescale communication. Reported cases of computer fraud are only part of the problem, considering employees pose a threat from the inside, Kesar says. "Lack of awareness of social and technical issues among managers largely manifest themselves in a failure to implement even the most basic safeguards and controls," Kesar writes. "Concomitantly, if management ignores wider organizational structural issues then this too increases the likelihood of a potential offender committing computer fraud."

Voting 2.0. Part 2: The Open Source Proposition
Linux Insider (05/30/08), K. Noyes

Stanford University professor and Verified Voting Foundation founder D. Dill says the trustworthiness of an electronic voting machine can only be ensured with a voter-verifiable audit trail, and his group currently recommends a system whereby voters fill out a paper ballot and place it into a scanner that also serves as a ballot box. The scanner counts or records the ballot, or gives the voter an opportunity to correct the ballot if it is mismarked. A bigger issue is whether any voting technology should be proprietary, and an open source voting system is being urged by groups such as the Open Voting Consortium, which believes that a paper trail alone cannot guarantee the transparency of all aspects of an election. An Ubuntu-based open

source system designed by the consortium is also voter-verifiable because it lets the public review in advance the screens they will see on Election Day, represented as pre-rendered picture files. Princeton University professor E. Felten says the public should be allowed to view the source code and comprehend the design of the technology, while less important is giving people the ability to modify the software. Dill acknowledges that an open source solution is desirable, although it is not a panacea by any means. "Open source can still be buggy and malicious, and it's also still very hard to know that that software is what the machine is actually running," he says.

To Make a Security Point, Hackers Tweak an Implantable Pacemaker
Sacramento Bee (CA) (05/17/08) P. A4; P. Dahlberg

A team of researchers has proven that with enough time, energy, and expertise a pacemaker can be hacked, though there is currently little to no risk for patients with pacemakers. Harvard cardiologist Dr. W. Maisel, who specializes in heart rhythms and was on the team, says hacking is not an important risk for patients right now, but that they just want the industry to be thinking about where society is going with such devices. Maisel worked with computer experts from the University of Massachusetts, Amherst, and the University of Washington to demonstrate that an implantable defibrillator could be accessed and altered remotely, possibly resulting in either a dangerous shock or the withholding of a potentially lifesaving one. The timing of the research is fitting, with a greater variety of implantable electronic gear being developed, particularly as the gear becomes more versatile and easier to operate from a distance. Pacemakers can send signals to bedside monitors to provide data for doctors, and some devices can be detected and reprogrammed quickly in an emergency room to help save a patient's life. UC Davis Medical School professor L. Wolff, who specializes in implanting defibrillators, says he believes in time it will be possible to make programming changes to implanted medical devices over the telephone. Researchers at the Medical Device Security Center tested a pacemaker in a lab, using $30,000 worth of commercially available equipment to assist with the hack, altering the device from less than an inch away.

Exploiting Security Holes Automatically
Technology Review (06/03/08), E. Naone

Researchers led by Carnegie Mellon University professor D. Brumley have found that software patches could be just as harmful as they are helpful because attackers could use the patches to automatically generate software in as little as 30 seconds that attacks the vulnerabilities the patch is supposed to fix. The malicious software could then be used to attack computers that had not received and installed the patch. Microsoft Research's C. Gkantsidis says it takes about 24 hours to distribute a patch through Windows Update to 80% of the systems that need it. "The problem is that the infrastructure capacity that exists is not enough to serve all the users immediately," Gkantsidis says. "We currently don't have enough technologies that can distribute patches as fast as the worms." This distribution delay gives attackers time to receive a patch, find out what it is fixing, and create and distribute an exploit that will infect computers that have not yet received the patch. The researchers say new methods for distributing patches are needed to make them more secure. Brumley suggests taking steps to hide the changes that a patch makes, releasing encrypted patches that cannot be decrypted until the majority of users have downloaded them, or using peer-to-peer distribution methods to release patches in a single wave.

Malicious Software Threatens Internet Economy

New Scientist (06/02/08), Ψ. Barras; T. Simonite

Malicious software is a growing threat to national economies and security interests, concludes an Organisation for Economic Co-operation and Development (OECD) report. The report says communities that fight malware only manage to offer a fragmented local response to what is a global threat, noting that about one in four personal computers in the United States, or 59 million PCs, is already infected with malware. Furthermore, a booming malware market is making it easier to launch cheaper and more sophisticated attacks. Zombie computers infected by malware are used to send out roughly 80% of all spam, and to attack commercial Web sites and other Internet-linked systems with crippling amounts of traffic as part of extortion schemes. Although the largest botnets have included up to 1 million computers, and the number of computers infected is increasing, OECD found that the number of computers in each botnet is actually shrinking to avoid detection. OECD says that international organizations and agreements are needed to properly measure and counteract the impact of malware attacks.