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

Δελτίο 130
30 Σεπτέμβρη 2008

Cyber Attack Data Sharing Is Lacking, Congress Told
Washington Post (09/19/08) P. D2; E. Nakashima

US intelligence agencies are unable to share information on foreign cyberattacks against companies due to a fear of jeopardizing intelligence-gathering sources and methods, testified P. Kurtz at the first open hearing on cybersecurity held by the House Permanent Select Committee on Intelligence. Kurtz and other cybersecurity experts discussed the Bush administration's Comprehensive National Cybersecurity Initiative, which focuses on cybersecurity espionage against government systems but, according to the experts, does not adequately address the private sector. The panelists, members of the Center for Strategic and International Studies commission on cybersecurity, say there is no coordinated strategy or mechanism for sharing intelligence about intrusions with companies, nor is there a systematic way for companies to share information with the government. Although certain information must be kept classified, the government needs to be better at sharing unclassified information on cyberattacks, says Rep. S. Reyes (D-Tex.), who chairs the intelligence committee. Office of the Director of National Intelligence's R. Feinstein says the intelligence community works very closely with law enforcement on cyberattacks to share knowledge that might assist with investigations, and with the Dept. of Homeland Security to assist with infrastructure protection efforts. Kurtz also says the US is heavily investing in technologies that are being stolen at little to no cost by the country's adversaries.

Electoral Apocalypse? e-Voting Woes Remain as Election Nears
Ars Technica (09/21/08), J. Sanchez

Two recent reports suggest that efforts to modernize the US electoral system are falling short of their objectives. The US Government Accountability Office (GAO) recently issued a report that summarized the findings of a year-long performance audit of the Election Assistance Commission (EAC), which was established by the Help America Vote Act of 2002 to help states upgrade their voting systems. The EAC is supposed to provide a federal-level certification process for voting systems. The EAC has 12 certifications pending, but none are finalized, meaning states must rely on their own procedures. The GAO report says the EAC has failed to "define its approach for testing and certifying electronic voting systems in sufficient detail to ensure that its certification activities are performed thoroughly and consistently." The problem of vague criteria and procedures appears to plague EAC in a variety of areas, the report says. The EAC has failed to establish an effective and efficient repository for certified versions of voting system software for states and local jurisdictions to use to verify that their voting systems match systems the EAC has certified. A second report, issued by the Century Foundation and the advocacy group Common Cause, notes that technological changes are presenting new difficulties for states. For example, in an electoral dry-run in Colorado earlier this year, officials discovered ongoing problems with lag and connectivity in the centralized voter registration systems used to check in voters with their local polling stations. Even when machines function properly, the Common Cause study found that user confusion with electronic systems could create a problem if states have not taken adequate steps to familiarize voters with the new machines.

US Focusing Cybersecurity on Backdoors in Tech Products
IDG News Service (09/15/08), G. Gross

Officials from the US Dept. of Homeland Security (DHS), the White House, and the Office of the Director of National Intelligence unveiled new details about President Bush's National Cybersecurity Initiative at a recent cybersecurity conference. Among the officials in attendance at the conference was DHS deputy secretary P. Schneider, who noted that the US government needs to better protect its supply chain from hidden vulnerabilities and Trojan horses in some commercial technology products made overseas. Some credit-card point-of-sale machines, for example, have stolen credit card numbers and passwords. Schneider noted that the government plans to work with private vendors to protect its supply chain, and will implement stringent acquisition rules for commercial technology products. In addition to addressing concerns about the supply chain, Schneider noted that the government is also planning to upgrade its perimeter defense scanner, Einstein. The system is largely a passive monitoring system that alerts the government that it has been attacked after the fact. The new version of the system will allow the government to anticipate where threats will come from and prevent cyber criminals from launching attacks. Officials at the conference also noted that the National Cybersecurity Initiative will focus on other issues, including improving the sharing of information about cyberattacks and sharing government defense capabilities with private companies.

reCAPTCHA: Human-Based Character Recognition via Web Security Measures
Science (09/12/08) Vol. 321, No. 5895, P. 1465; L. von Ahn; B. Maurer; C. McMillen

The reCAPTCHA project employs CAPTCHAs to help digitize scanned typeset texts by having people decipher the words that computers are incapable of recognizing, says Carnegie Mellon University's L. von Ahn and colleagues. CAPTCHAs are distorted word puzzles that humans can successfully solve but current computer programs cannot, and they are used to prevent the abuse of online services by automated programs. Von Ahn notes that recapTCHA "is used by more than 40,000 Web sites and demonstrates that old print material can be transcribed, word by word, by having people solve CAPTCHAs throughout the World Wide Web." ReCAPTCHA provides the user with two words, the one for which the answer is unknown and a second "control" word for which the answer is known. A correctly typed control word causes the system to assume that the user is human and confidently conclude that he also typed the other word correctly. ReCAPTCHA accounts for human error in the digitization process by sending every unrecognizable or suspicious word to multiple users, each time with a different random distortion. The authors have learned from a large-scale implementation of the reCAPTCHA system that deciphering words using CAPTCHAs can match the highest-quality guarantee provided by dedicated human transcription services. Von Ahn and colleagues conclude that reCAPTCHA clearly shows that "'wasted' human processing power can be harnessed to solve problems that computers cannot yet solve."

Eugene Spafford: Protecting the Internet From the Criminal Element
Science News (09/13/08) Vol. 174, No. 6, P. 32; S. Gaidos

The nature of computer security incidents has changed dramatically in the past three decades, says E. Spafford, executive director of Purdue University's Center for Education and Research in Information Assurance and Security and chair of ACM's US Public Policy Committee. He recalls that while most incidents in the 1990s were mainly perpetrated by people who were either adjusting to the unfamiliarity of the Internet or were "classic hackers" out for bragging rights or to demonstrate their skills to others, today's hackers are more sophisticated and committed to true criminal enterprises, including credit card fraud and the theft of information and intellectual property. The network is now global in scope, which increases its exposure to individuals with a wide spectrum of motives and ideologies, Spafford says. He says the Internet is devoid of an effective policing framework, given its lack of physical boundaries. Redressing the absence of computer security requires society to become more willing to pay for good security and less tolerant of flaws and security incidents, Spafford argues. "We have to find ways to increase accountability, authenticity, and attribution without doing away with some of the freedom of expression that is part of the benefit of having the Internet," he says. "The probable direction we're going to have to go in is to build very robust, highly protected enclaves, or protected systems of computers."

US Urged to Go on Offense in Cyberwar
United Press International (09/29/08), S. Waterman

The United States needs to do more to develop its offensive cyberwar capabilities rather than focus solely on defending its networks from attack, says Rep. J. Langevin (D-R.I.), the chairman of the House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. Langevin called on the White House to declassify more of its Comprehensive National Cybersecurity Initiative and said the Dept. of Homeland Security should be relieved of its lead role in defending the nation's computer networks. "Never again will we see major warfare without a strong cyber component executed as part of it," he says. Langevin's call to cyberarms highlights a debate in government surrounding how best to address the complex challenges posed by the US's dependence on the Internet and other computer networks, which could provide an exploitable vulnerability. A major issue analysts emphasize is the difficulty in determining the origins of cyberattacks. Former White House cybersecurity official P. Kurtz has said that until the US is better able to identify the origin of an attack, it is going to be very difficult to contemplate a military option and to respond appropriately. Another issue is that for any offensive capabilities to be a deterrent for adversaries, the US military's cyberwar capacities would have to be made public. "As part of an overall doctrine and strategy in cyberspace, we need to consider what are the deterrent factors," says former assistant deputy director at the National Security Agency J. Nagengast.

Conference Will Key on Improving Internet Security
New Brunswick Business Journal (Canada) (09/29/08), D. Shipley

The Sixth Annual Conference on Privacy, Security and Trust (PST), which takes place this week in New Brunswick, Canada, will bring together security experts from around the world to discuss ways of improving Internet privacy, security, and trust. Co-hosted by the University of New Brunswick (UNB) and the National Research Council, the PST conference will focus on finding innovative ways of ensuring that information is secure and private. "The more new technology, particularly in the information, communications, and technology sector (ICT), and the more information we process over this ICT infrastructure, the more we have to deal with the security of that infrastructure and the security of information on that infrastructure," says UNB professor and PST 2008 conference chair Ali Ghorbani. Ghorbani says that although some security systems have improved, dealing with IT-based security and privacy is a never-ending battle. Threats on the Internet are as diverse as the Web itself, and increasingly includes national governments looking to engage in a new form of warfare. "This is going to be part of any bad guy's agenda in the future because it can be done in anonymity," Ghorbani says. "It is something that should be a concern." The PST conference will cover such topics as network and wireless security, anonymity and privacy versus accountability, and critical infrastructure protection.

Spoofing GPS Receivers
Cornell News (09/19/08), A. Ju

Cornell University researchers have shown that global positioning system (GPS) technology is vulnerable to spoofing, or transmitting fake signals that receivers believe are authentic. At a meeting of the Institute of Navigation in Savannah, Ga., the researchers presented a paper that described how a phony GPS receiver was placed near a navigation device, and tracked, modified, and retransmitted the signals from the system of satellites circling the Earth. The navigation device eventually mistook the false signals as real signals. The team says a GPS attack would have a serious impact considering how ubiquitous the technology has become. "Our goal is to inspire people who design GPS hardware to think about ways to make it so the kinds of things we're showing can be overcome," says Cornell professor M. Psiaki. The US government described seven countermeasures for a GPS attack in a December 2003 report, but the Cornell team says they would not have foiled its reprogrammed receiver. "We're fairly certain we could spoof all of these, and that's the value of our work," says Cornell researcher T. Humphreys.