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

Δελτίο 27
7 Μάη 2006

Guidelines For Radio Tags Aim to Protect Buyer Privacy
New York Times (05/01/06) P. C6; B. Feder

New guidelines are being released during a technology trade show in Las Vegas to protect consumer privacy when identification and tracking systems that use small radio tags are used. RFID technology is becoming more common in libraries, hospitals, and systems that track consumer goods through the retail supply chain. The guidelines say consumers should be notified when products have radio tags and that consumers should know how to disable disposable forms of the tags easily. Procter & Gamble, IBM, Microsoft, Visa USA, and the National Consumers League are some of the participants expected to endorse the guidelines. Some opponents of the guidelines include the National Retail Federation and the Electronic Frontier Foundation (EFF). EFF lawyer L. Tien says the guidelines give the industry too much room and ignore government use of RFID along with privacy concerns for employees in business-to-business dealings. A survey last year found that 7% of 89 retailers and 11% of 120 consumer products manufacturers had delayed or cut back RFID investments over privacy concerns, according to C. Overby at Forrester Research. RFID is currently used in wireless toll collection systems and to control access to buildings, track livestock, and manage industrial assets.

New Weapons Needed for the War on Junk Email
University of Calgary (04/27/06)

Spam filters may be highly effective, but they cannot keep up with spammers who are coming up with new ways to trick people into visiting commercial Web sites or downloading rogue software carrying viruses, worms, spyware, or other dangerous applications, according to J. Aycock, an assistant professor of computer science at the University of Calgary. Aycock and his student Nathan Friess performed research that shows it is possible to create a new type of spam, or bulk email, that can go past the best spam filters and trick even the most advanced computer users. Aycock and Friess will present their research during the 15th annual conference of the European Institute for Computer Anti-Virus Research, being held in Hamburg, Germany, on April 30. The goal of the research is to increase awareness of the threat so that anti-spam software that anticipates what spammers will do next can be written. "We want to look at potential threats and see what we can do about them right now, as opposed to getting to the point where we're forced to react," says Aycock. The majority of spam today is sent from zombie computers, which can automatically send large email messages. Aycock predicts that spammers may soon use zombie computers to tap into a person's email account, which was previously thought of as too complex, but research shows that is now possible. Aycock wants companies that make anti-spam software and email programs to take advantage of the new information and use the suggested solutions in their existing software suites.

RFID and Tracking Systems--The High-Tech Future of Old Age?
silicon.com (04/27/06), S. Ranger

New gadgets and computer monitoring systems are focusing on the elderly, allowing those without an extended family to live at home as long as possible. Several such products are being tested at Accenture's Technology Labs in Sophia Antipolis, France. Among these are camera systems that follow the elderly around and call for help if they fall. These systems can be used to monitor activity levels and eating habits as well. An RFID-equipped online medicine cabinet is also in the works, alerting seniors if they choose the wrong medicines. Interactions with relatives and caregivers, meanwhile, are encouraged with the "connective table," which allows users to play board games and look at important documents via camera sensors and video projectors. Accenture researcher A. Opalach says that by 2020 there will be twice as many people 65 or older than there are today. Opalach says "this demographic change is going to have an impact. Technology can help people stay independent for as long as possible."

Better Organization, Focus Needed for Cybersecurity
Government Computer News (04/27/06), W. Jackson

The US government needs to create clear lines of authority and clarify responsibility for an effective national information assurance policy, according to former presidential adviser P. Kurtz, who is now executive director of the Cyber Security Industry Alliance. "We have a growing body of law and regulation bearing on information security," said Kurtz during the GovSec conference in Washington on Thursday. "We are not ready for a major disruption of the information infrastructure today, and we have a long way to go to get there." Kurtz suggested a two-tiered framework for cybersecurity where critical functionality could be identified for government attention, and less important issues are given to the private sector. Kurtz and T. Leighton at Akamai Technologies agree that cyberspace is getting tougher and that an infrastructure needs to be built to better respond to possible attacks. An assistant secretary for cybersecurity is still needed in order to establish an effective policy, according to Kurtz. The position has been vacant for almost a year now.

Bugs Put Widely Used DNS Software at Risk
IDG News Service (04/26/06), R. McMillan

University of Oulu researchers say they found multiple flaws in the software used for administering the Internet's Domain Name System (DNS), which may cause several problems such as crashing the DNS server or giving attackers a way to run unauthorized software. Oulu researchers have come up with a DNS test suite to test for such vulnerabilities. Microsoft, Cisco Systems, and Sun Microsystems are currently testing their products, but there is no word yet on whether customers will be affected. DNS servers have come under fire lately because of such attacks, which may compromise the DNS system and take down several Web sites. Just last month, unknown attackers used computers and DNS servers to spread denial-of-service attacks against about 1,500 organizations, according to VeriSign.

New Software Protects Confidentiality of Data While Enabling Access and Sharing
Penn State Live (05/01/06)

Penn State researchers presented the paper "Privacy-preserving Semantic Interoperation and Access Control of Heterogeneous Databases" at the recent ACM Symposium on Information, Communication and Computer Security in Taiwan. In the paper, the researchers describe the development of new software that allows databases to communicate with each other without jeopardizing the security of their data and metadata. The Privacy-preserving Access Control

Toolkit (PACT) is designed to act in the manner of a filter by encrypting queries, data communicated, and other information. "The software automatically regulates access to data, so some information can be exchanged while other data remains confidential and private," explained P. Mitra, assistant professor of information sciences and technology at Penn State. "Often when we implement security, we decide not to give access to data." The researchers took a more generic approach to designing PACT compared with the special-purpose applications that organizations develop for sharing data, which are expensive, take more time to develop, and do not address security issues. Research on PACT will continue with the development of a new rule language to enhance interoperability as well as improvements to boost the performance of query processing.

Big Holes in Net's Heart Revealed
BBC News (04/28/06), M. Ward

Cornell University researchers have found that the Web's addressing system is archaic and needs patching if not replacement. In a study of some 600,000 computers, the researchers found that more than a third of Internet sites are susceptible to simple attacks--a number that could increase to 85 percent if a more sophisticated denial-of-service attack were launched concurrently--due to the Net's reliance on an average of 46 computers each holding different information about the components of a net address that must be consulted when a site is visited. This chain of dependency creates vulnerabilities. "The growth of the Internet has caused these dependencies to emerge," says computer science professor E.G. Sirer of Cornell. "Instead of having to compromise one you can compromise any one of the three dozen...The domain name system has been incredibly successful so far but it is showing its age. We need to re-think the entire naming infrastructure of the Internet." One solution would involve utilization of a peer-to-peer type structure for domain addresses. The research also found that 17% of the servers that host Net address books are vulnerable to attack from well-known threats. Sirer says, "Because of these dependencies about one-third of the Net's names are trivially compromisable by script kiddies." For example, Sirer found that one of the five computers that act as the first reference point to the fbi.gov domain still has not been patched to protect against a common bug. Although the FBI fixed the problem once informed, Cornell researchers say hundreds of thousands of sites remain vulnerable.

RFID Standards Released IT by Vendors, Privacy Groups
IDG News Service (05/01/06), G. Gross

A group of technology vendors, radio frequency identification (RFID) users, and consumer groups issued a series of best practices about RFID tags on Monday to allay consumers' worries about the technology. Privacy advocates have warned that RFID could facilitate corporate and government surveillance of people's movements and transactions as the technology's scanning capabilities become wider-ranging. The Center for Democracy and Technology's (CDT) Working Group on RFID recommends that companies using RFID tags notify customers in all cases, tell customers if they can turn off the tags, and embed security. In addition, the group advises companies that collect personally identifiable data via RFID tags to disclose how that data will be employed to customers; the working group's best practices report says options for customers to opt out of sharing personally identifiable information and to destroy the tags "must be readily available." The report goes on to say that "consumers should know about the implementation and use of any RFID technology...[but] it is important to recognize that notice alone does not mitigate all concerns about privacy." According to the CDT report, companies using RFID should give customers "reasonable" access to the information collected by the tags, and should notify customers of their RFID use prior to the completion of transactions. "These new guidelines show how RFID can provide great benefit to society, while treating customers' privacy with respect," declared Microsoft researcher S. Shafer.