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

Δελτίο 34
25 Ιουλίου 2006

Tech Researchers Creating Software to Protect Children
Roanoke Times (VA) (07/15/06), A. Manese-Lee

Researchers at Virginia Tech are developing software designed to verify that a Web site has the parental consent to begin collecting information on their children. The POCKET (Parental Online Consent for Kids' Electronic Transactions) software is designed to make it easier for parents to guard against Web sites that request information from their Web-surfing children. "Right now, every single Web site that the child goes to that wants to collect information, they are required to go get their parent, bring their parent to the computer, and, through several methods depending on what the Web sites are doing with the information, get the parent to consent for the child to enter the information," explains J. Hiller, professor of business law at Va. Tech's Pamplin College of Business. "This system is like an agent for the parent." Parents and Web sites must contribute to POCKET for the software to be effective. POCKET has parents fill out a privacy preference form on what information, from the full name of their child to their street address, is okay to be shared, and Web sites fill out a similar form that details the information they collect. The software will allow a child to connect to a Web site if it does not ask for more information than the parent has entered into a privacy preference form. POCKET is the focus of a three-year project that received $450,000 from the National Science Foundation Cyber Trust program last year, and the researchers have several issues to address as they continue to develop the software, such as how to effectively authenticate parental registration and how to block only a certain part of a Web site where more information is requested.

Voting Software
Embedded.com (07/17/06), J. Ganssle

With the November elections fast approaching, the uncertainties that still pervade the multitude of e-voting systems in use throughout the country will likely result in the candidates who lose tight races crying foul, writes J. Ganssle. The machines are not the only part of the process that is suspect, according to a recent ACM report on the software used to register voters. "In light of recent events and legislation that have underscored the core importance of voting and of public confidence in our electoral system, one might conclude that all VRDs should be built and operated to the highest possible standards. While the highest standards of reliability, privacy, accountability, usability, and security are desirable, they may be impractical because of resulting expense or system response," report reads. What ACM describes as "system response" is merely a subterfuge aimed at convincing the non-technically inclined that good code is too slow, and that the only code that will run fast enough will be plagued with glitches. ACM recommends testing, though Ganssle claims that most tests only inspect half the code, and that it is more important to look at the internals of the system. While e-voting will ultimately lead to a faster and more secure election process, as well as opening the door to more absentee votes, the machines must be built on an operating system that has been certified and vetted by the open-source community.

Experts Tell Congress U.S. E-Voting Security Is Flawed

EE Times (07/19/06), G. Leopold

E. Spafford, chairman of ACM's Committee on Public Policy, told a joint House hearing Wednesday that ACM has concerns about the federal qualification process for computerized voting technology. US standards for voting equipment are voluntary, but application of the federal specs has been inconsistent, according to a recent report from the Government Accounting Office. Meanwhile, critics of electronic voting machines say they can be hacked into to compromise elections. "New federal standards and a certification process hold promise for addressing some of these problems, but more must be done to ensure the integrity of our elections in the face of software and hardware errors as well as the possibility of undetectable tampering," said Spafford. Clear security standards would be helpful because they would reduce the number of designs, according to a list of steps to shore up accuracy and security released by Spafford. A more transparent testing process, a mechanism for periodic security updates, and voter-verified paper trials are the other steps.

Feds Sharpen Secret Tools for Data Mining
USA Today (07/20/06) P. 5A; M. Kelley

Since the Sept. 11, 2001, attacks, US intelligence agencies have spent millions of dollars on software to form connections between previously unknown people and terror suspects, track the flow of money through international financial institutions, and monitor global communications. The actual cost of Pentagon and CIA data-mining programs is classified. At least five such programs were developed under the Pentagon's now-defunct Total Information Awareness (TIA) program. Congress scrapped the program three years ago out of privacy concerns, but the Bush administration claims that citizens' privacy is protected under the current surveillance programs. Privacy advocates worry the administration's claim that counterterrorism is a legitimate use for warrantless surveillance is the first step down a slippery slope. "There's a tendency with all of these systems to lead with terrorism and then find other applications," said M. Rotenberg, executive director of the Electronic Privacy Information Center. Among the data-mining technologies in use by intelligence agencies are hardware that can search through databases up to 4 million GB, a program aimed at identifying terrorist networks and the most important members within those networks, and software containing personal information about Americans compiled by other agencies and commercial groups. At least eight TIA projects, including the five data-mining initiatives, have continued since Congress pulled the plug on the program in 2003. The law dismantling TIA allowed research to continue in some areas, including the development of two computer simulations to test a variety of counterterrorism situations. Supporters claim the TIA's data-mining programs could be continued under the exemptions, while critics warn of a lack of accountability.

Surveillance Bill Meets Resistance in Senate
Washington Post (07/21/06) P. A9; D. Eggen; C. Babington; J. Eilperin

Democratic senators and national security experts opposed a Senate surveillance bill proposed by Sen. A. Specter (R-Pa.) that would permit the Bush administration to submit the National Security Agency's (NSA) warrantless eavesdropping program to a clandestine intelligence court so that its legal ramifications can be assessed, arguing that the legislation would extend the government's powers to monitor Americans without being watchdogged by the courts. The NSA program allows the agency to eavesdrop on emails and phone calls between the United States and overseas locations without court sanction if one of the parties is believed to have terrorism links. Specter's bill would allow all pending lawsuits related to the NSA program to be transferred to a secret Foreign Intelligence Surveillance Act (FISA) ap-

peals court that could dismiss the cases "for any reason," and permit the White House to seek the legal okay for the NSA program from another secret FISA court. In addition, the bill would extend the length of time the government could monitor alleged terrorism suspects before getting warrants, and would categorically assert the president's "constitutional authority" to undertake spying programs by himself. Critics complain that the legislation would eviscerate the FISA law and allow the government excessive latitude in secret surveillance, as well as let the FISA court approve surveillance in its entirety instead of evaluating warrants for particular cases. Meanwhile, House GOP leaders Reps. P. Hoekstra (R-Mich.) and F.J. Sensenbrenner Jr. (R-Wis.) are endorsing a competing bill. All GOP proposals that address the NSA issue are opposed by Rep. J. Harman (D-Calif.) on the House intelligence committee, who said the bills are "solutions in search of a problem."

Department of Homeland Security Establishes Center at Illinois
University of Illinois at Urbana-Champaign (07/19/06)

Working under a three-year, $2.4 million grant from the Department of Homeland Security, researchers at the University of Illinois will develop applications capable of processing vast quantities of data in a variety of formats. Illinois is sharing a $10.4 million grant with researchers from the University of Southern California, University of Pittsburgh, and Rutgers University. The grant will help Illinois establish the Multimodal Information Access and Synthesis (MIAS) Center. "The MIAS will advance the understanding and technologies required to deal with large amounts of information available today in multiple text forms," said D. Roth, professor of computer science at Illinois and the director of the center. "The center builds on department of computer science strengths in such areas as machine learning, natural language processing, information retrieval, image processing, databases, and data mining." In the coming years, scientific research will produce huge amounts of multimodal information that will require systems capable of interpreting and analyzing data in multiple formats, developing and verifying hypotheses, and incorporating observed data into domain names. Though their work is commissioned by DHS, the researchers expect the MIAS center to produce technologies that will also have significant impact on the business community. The center will also include a summer school for undergraduate and graduate students. "Altogether, the overarching goal is to use science and technology to reduce threats to our nation's security by providing new knowledge and cutting edge technology and by helping produce a growing number of professionals through our educational programs," Roth said. "It will also have significant impact on the growing industry of information access, search engines, and mining knowledge from data."

RFID Privacy Concerns Spark a Closer Look by a U.S. Senate Panel
Investor's Business Daily (07/18/06) P. A4; J. Bonasia

A bipartisan Senate panel headed by Sens. B. Dorgan (D-N.D.) and J. Cornyn (R-Texas) last week convened for the first time to address the future of radio frequency identification (RFID) technology and related privacy concerns. Commonly used now to track goods, the technology could one day be a mainstay of commerce, utilized much like barcodes are today. But RFID technology can store much more than just product information and can be scanned from a distance. Privacy advocates have expressed concern that the technology could leave consumers exposed to tracking and are calling for RFID sensors to be disabled at the point of sale. States have begun to implement their own measures to address such worries. Wisconsin in May passed a measure that makes it a crime to require a person to be implanted with an RFID chip for security clearance purposes. Thirteen states or more are considering similar

controls on the use of the technology. Dorgan and Cornyn would like to see guidelines for use set at the federal level without threatening the US lead in RFID technology R&D.