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

Δελτίο 63
28 Φλεβάρη 2007

Campaign Strengthens for a Voting Paper Trail
Washington Post (02/19/07) P. A17; Z. Goldfarb

Independent audit measures for e-voting are gaining momentum in Congress. The Democrats that now control Congress appear to be dedicated to proposed e-voting bills that would require printouts and tests of paper tallies against electronic results. The bill introduced in the House has almost 200 co-sponsors. "We are closer now to paper-trail legislation than we have ever been before," says Electionline.org's D. Chapin. Currently, 27 states require e-voting machines to produce paper trails. However, requiring a paper trail could bring about new problems "in terms of both creating post-election litigation and creating administrative problems in counting these paper strips," says Ohio State University's election-law program director D. Tokaji. "We know they can be compromised, torn, crumpled," and experience various printing problems, he adds. In addition to changes in election day practices, the Election Assistance Commission (EAC) will increase scrutiny of the process for testing voting machines prior to elections: Evaluation of testing labs will now include the NIST. "It's the first time the federal government has ever been involved in testing voting equipment and, with NIST recommending their accreditation, that puts a more stringent position on the labs to meet all of the qualifications," said EAC chair D. Davidson.

Europe's Plan to Track Phone and Net Use
New York Times (02/20/07) P. C4; V. Shannon

Germany and the Netherlands are preparing legislation that would require companies to keep data concerning customer's Internet and phone use in a manner that would go beyond the requirements of the European Union Data Retention Directive, which must be put into law by all member countries by 2009. Germany would make it illegal to open email accounts using false information, and the Netherlands would mandate that phone companies save information on the exact location of a customer during a phone conversation. Current EU law requires that Internet service providers, who keep customer information for months for billing purposes, disclose this information in the case of valid legal investigations. The proposed German email law states that email aliases are only legal if they are traceable to the account holder. "This is an incredibly bad thing in terms of privacy, since people have grown up with the idea that you ought to be able to have an anonymous email account," says European privacy counsel for Google P. Fleischer. He also points out that the law would have to implement some sort of identity verification system. However, European law may not apply to US-based email providers, making it very easy for Europeans to use a fictitious account. When the EU directive was announced, Internet and telecom groups debated the length of time information must be stored and how companies would be compensated for the costs of this retrieval and storage, so the directive ended up leaving these decisions to individual countries.

World Leading Human Behaviour Experts Awarded Security Study Contract
Innovations Report (02/16/07), B. White

The human factor in securing computer systems will be the focus of a new study funded by the UK government's Cyber Security Knowledge Transfer Network (KTN). M. A. Sasse, professor of Human-Centered Technology at UCL, will head the diverse team of researchers that will include specialists in computing as well as psychology, criminology, management, and marketing. Computer security pioneer F. Piper, security experts from industry and academia, software engineering researchers, and human behavior specialists will all be involved in the project. In the spring, the team will present a white paper with best practices and recommendations for protecting PCs and UK critical infrastructure from cyber attacks and organized e-crime. "Vulnerabilities introduced by human behavior are often at the heart of security problems and I expect this team to make a valuable and practical contribution to the community's understanding of this important issue," says Dr. S. Creese, director of the Cyber Security KTN. "The IT security community has given only patchy consideration to the human factor in security and I welcome the opportunity to help improve our collective understanding of this critical area and translate it into practical advice for companies and individual users."

US Cybersecurity Czar Has His Marching Orders
CNet (02/20/07), J. Evers

In his capacity as US cybersecurity czar, G. Garcia plans to formulate strategies for promoting the adoption of security technologies through tax breaks and other incentives, as well as encourage cooperation between the public and private sectors by establishing links between federal security watchdogs and their private industry equivalents. He says in an interview that he is aiming for "a more concerted effort, a series of hearings that really look at some of the different critical infrastructure sectors ... to articulate how it is that investing in security is going to accrue more benefits back to the company." Garcia explains that his title and role as DHS assistant secretary has been a boon by virtue of the authority vested in it, which is key to moving things forward. He notes that he has confidence that his plan will be successfully implemented because "I've got my leadership team in place, and so I'm feeling much more complete as an organization that we have the intellectual firepower [and] we have people with years of government experience who understand how to get things done." Garcia says his goal is to promote proactive rather than reactive consideration of customer-driven security through a raising of awareness; he suggests that Congress could modify laws to fuel investment. The cybersecurity czar foresees the funneling of all global communications over a single pipeline based on Internet Protocol, and asserts that efforts should be made to determine such a system's weaknesses and embed security while the architecture is in development. The presence of a global supply chain also calls for built-in security procedures, Garcia says.

Security Experts Draw Bead on How Malware Targets and Dupes Internet Users
Indiana University (02/19/07)

As cyber crooks focus more of their attention on consumers, security experts are questioning what role Internet users play in becoming victims of malware attacks. Security researchers and practitioners addressed the issue during the symposium, "Malware: The Next Big Internet Threat," during the recent annual meeting of the American Association for the Advancement of Science. "It's only recently that researchers and security practitioners have recognized the human factor of Internet security, and criminals already have established an advantage," says M. Jakobsson, associate professor at the Indiana University School of Informatics. They now realize that programs are not always configured correctly, consumers do not always use programs the right way, and users do not always heed securities warnings, says Jakobsson, who is also associate director of the Center for Applied Cybersecurity Research at

IU. He also says the emergence of phishing shows that cyber criminals are focusing on tricking consumers. Jakobsson participated in the Feb. 18 panel that discussed the economic forces behind malware, how cyber criminals launch the attacks, and how to guard against them.

Panel Cites Voter Error, Not Software, in Loss of Votes
New York Times (02/24/07) P. A9; C. Drew

A team of computer experts from several universities has announced its unanimous decision that there is no evidence supporting the argument that voting machine malfunction was to blame for the undervote in the 2006 Sarasota County Congressional race. Possible explanations offered by the team, which was lead by Florida State University computer science professor A. Yasinac and University of California, Berkeley professor D. Wagner, were that voters could have touched the screen twice, erasing their own vote, or could have missed the race entirely, due to poor ballot design. The race did not have the colorful heading that others did, was sandwiched between long lists of candidates for the Senate and Governor elections, and was squeezed in at the top of a screen. Wagner said, "I'm persuaded that this wasn't caused by machine failure." However, in the days following the election, a local paper reported several voters complaining that although an "x" appeared in the box for C. Jennings when they touched it, the "x" was gone when they reached the verification screen at the end of the ballot. The report did indicate that aging hardware could have been responsible for isolated problems, but such problems would have also impacted other races. This investigation marks the first time software code has been audited to resolve an election, but some computer experts are not satisfied. "The study claims to have ruled out reliability problems as a cause of the undervotes, but their evidence on this point is weak, and I think the jury is still out on whether voting machine malfunctions could be a significant cause of the undervotes," says Princeton's E. Felten.

Surveillance Cameras Get Smarter
Associated Press (02/25/07), S. Manning

The next generation of surveillance cameras are incorporating "intelligent video" technology in order to not only observe but interpret the images they capture. Cameras used in Chicago and Washington, DC, can detect gunshots and call police, while cameras deployed in Baltimore can play a recorded message and take pictures of illegal dumpers or graffiti artists. Intelligent video technology can analyze a person's gait, for example, to determine whether a person may be concealing a weapon, and it can even recognize faces. "If you think of the camera as your eye, we are using computer programs as your brain," said the Army Research Lab's P. Gillespie. University of Maryland engineering professor R. Chellappa and a team of graduate students have created a system that can both watch for changes in an environment based on what it is programmed to see as "normal," and track people who cross established perimeters. The system places a box around the suspicious person or object on a computer display and alerts security to evaluate the threat. One exhibition showed the system recognized a suspicious person who got out of his car in a garage and went from car to car, looking in the windows, and placed a box around him as he moved. However, before intelligent video technology makes it to the market, the technology needs to be improved, and liability issues must be worked out. Ultimately, Chellappa wants to develop systems that can see what someone might be concealing and actually stop some threats.

Homeland Security Cyber Czar Sees Challenges Ahead

National Journal's Technology Daily (02/22/07), H. Greenfield

Cyber threats reported to the U.S. Computer Emergency Readiness Team increased from 5,000 incidents in 2005 to 23,000 incidents in 2006, and there have already been 19,000 reports of cyber attacks in 2007. Homeland Security cyber czar G. Garcia said groups vulnerable to cyber attacks are interdependent and need to establish a level of trust and share information on vulnerabilities and threats. In an interview with National Journal's Technology Daily, Garcia outlined three broad goals to increase security. Those objectives are to strengthen information sharing, create stronger network security within federal agencies, and establish sector-specific infrastructure protection plans, as about 90 percent of critical infrastructure belongs to organizations in the private sector. Garcia also said U.S. CERT and the National Coordination Center, which is responsible for monitoring disruptions in the telecommunications network, will soon be housed under one roof, but the location was not disclosed for security reasons. Garcia said that although globalization of the world's technology industry will provide more opportunities, it also creates new security challenges, as does the move to a single, integrated Internet protocol. He says, "There are cost savings, productivity enhancements, but it also introduces a new level of vulnerability in our networks."