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

Δελτίο 18
4 Απρίλη 2006

Touch-Screen Voting Isn't the Answer
Baltimore Sun (03/31/06) P. 11A; J. Schneider

In framing the electronic voting-machine debate in Maryland around security, many experts are missing the point, writes John Schneider, an Internet and data security consultant. Because any system can technically be rigged or manipulated, security is a relative term, generally a function of the effort and risk of breaking into a system weighed against the rewards of doing so. Without a sufficient recovery plan, voters will have to take on faith from a small group of technologists that their votes have been counted and recorded accurately. Most involved in the debate agree that some kind of paper recording mechanism is in order so voters can confirm their choices. Paper ballots also enable officials to conduct a hand recount if the machines experience problems. One type of paper trail would feed a roll under glass for voters to lean forward and read, while another would have the voter create an individual ballot to be read by an optical scanner. Schneider writes that the critical difference between optical scanners and touch-screen systems is that voters prepare a ballot by hand with an optical-scan system so it cannot be hacked should a recount be necessary. Given the value of Maryland's inventory of touch-screen systems, an optical-scan voting system could be deployed for a net cost of around zero while offering the invaluable benefit of restoring confidence in the state's voting process, Schneider concludes.

Device Warns You if You're Boring or Irritating
New Scientist (03/29/06), C. Biever

Researchers are scheduled to present a device that will inform people with autism that they are boring or annoying the person they are talking to at next week's Body Sensor Network conference at the Massachusetts Institute of Technology. The "emotional social intelligence prosthetic" device is an improvement from previous computer programs that detect the basic emotional states of happiness, sadness, anger, fear, surprise, and disgust because it focuses on the more complex states of agreement, disagreement, concentration, thinking, uncertainty, and interest, which appear more frequently in conversation. Built by R. El Kaliouby of MIT's Media Lab, colleagues R. Picard and A. Teeters, with P. Robinson of the University of Cambridge, the device consists of a camera (small enough to be attached to eyeglasses) connected to a handheld computer that uses image recognition software, and software that can read the emotions of the images. The software makes the handheld vibrate when its wearer does not engage the listener. The device, which gets emotions right 64% and 90% of the time when presented with video footage of ordinary people and actors, respectively, is based on a machine-learning algorithm that was trained by showing it more than 100 eight-second video clips of actors expressing different emotions. The researchers say they still need to reduce the device's computing demand for a standard handheld, find a high-resolution digital camera that is easy to wear, and train autistic people to use it. In addition to autistic people, teachers could benefit from the device.

Researchers Cooperate to Create Better Ways of Finding Reliable Information Online
Chronicle of Higher Education (03/29/06), V. Kiernan

R. Lankes, an associate professor of information studies at Syracuse University, and M. Eisenberg, a professor in the University of Washington's Information School, want to make it easier for Internet users to find credible information online. The two researchers have received a two-year, $250,000 grant from the MacArthur Foundation to build a Web site, Credibility Commons, which will offer computer programs to help Web users assess the credibility of information they find online. Lankes says librarians, college instructors, and other information specialists continue to note that the quality of information online varies tremendously, and that they are more likely to trust information if a site has a professional appearance. Lankes adds that users are more likely to believe information if it is in line with their own thinking. As co-directors of the project, Lankes and Eisenberg are considering developing a search engine that would direct users to the Web sites used by skilled searchers, such as reference librarians. Although software developed by Credibility Commons would be available for free at the project's Web site, anyone who creates software based on the work of Lankes and Eisenberg would have to share their new application as well. "If you use it, you've got to share what you used it for," says Lankes.

Everything, Everywhere
Nature (03/23/06) Vol. 440, No. 7083, P. 402; D. Butler

Tomorrow's computers could be networks of minute, low-cost sensor nodes with built-in data processing and transmission capabilities; by constantly monitoring environments, buildings, and even the human body, these networks could usher in a transformation in the field of science. "We will be getting real-time data from the physical world for the first time on a large scale," says University of Washington computer scientist G. Borriello, noting that this will facilitate a paradigm shift in which theories can be generated and tested much more rapidly. R. Detrick with the National Science Foundation's Ocean Observatories Initiative (OOI) explains that sensor webs will allow researchers to integrate inputs from diverse sensors interactively and build "virtual observatories." Programming a sensor web for a specific scientific application is currently a formidable challenge, given the customization effort. Center for Embedded Networked Sensing director D. Estrin says scientific fieldworkers must contend with major sensor-web shortcomings: The price of sensors currently precludes the node densities researchers frequently need to conduct detailed field tests, while not all monitoring requirements can be fulfilled by sensor webs alone. Estrin projects that sensor webs will often function as just one tier in a stack of data collecting systems, and machine-to-machine communication will be needed on a grand scale to manage these stacks, thus necessitating the development of new operating systems and standards. Sensor-web tools will have to become more user-friendly if they are to break out of niche applications, according to Dust Networks founder K. Pister.

The Spies Inside
InformationWeek (03/27/06)No. 1082, P. 34; E. Chabrow

Law enforcement officials, IT professionals, and industry watchdogs are taking new approaches to controlling PC adware and spyware, as past efforts have yielded few effective measures. Organized criminal groups are involved in much of the spyware designed to steal individual identities, money, and trade secrets, according to Chris Painter with the US Justice Department. Spyware is a problem with an international scope, and is harder to curb because much of the malware installed on PCs hails from nations where virtual crime is a great temp-

tation to skilled but underemployed people. Adware, meanwhile, is employed to track users' Web habits for marketing and advertising purposes, sometimes without users' consent; critics draw little if any distinction between adware and spyware, given the surreptitious nature of both, according to Overstock.com's Jonathan Johnson. The threat of adware and spyware is prompting PC users to exercise more caution when surfing the Web or trying new software. FTC action against adware company 180solutions was requested by the Center for Democracy and Technology in January on the grounds that the company repeatedly and intentionally attempted to trick Internet users into downloading intrusive software. 180solutions paid Web publishers or affiliates to distribute the software without adequate oversight to make sure installation proceeded only when user permission was secured; 180solutions claims it spent $2.5 million on software to deter this practice, but the software is not foolproof. Criticism from the likes of the Center for Democracy and Technology may spur adware to reform such deceptive methods and attain a measure of legitimacy as an advertising medium, eventually becoming a workable tool for people to access free content.

Seeking Changes to the DMCA
CNet (03/31/06) Broache, Anne; D. McCullagh

The entertainment industry has been lobbying the US Copyright Office to head off changes to the controversial Digital Millennium Copyright Act (DMCA) of 1998 that security experts have been pushing for to protect their research. Princeton University computer science professor E. Felten said that he and J. Halderman, a graduate student, discovered the Sony rootkit vulnerability a month before it became public knowledge, but were unable to come forward for fear of a lawsuit under Section 1201 of the DMCA, which prohibits such a disclosure without the authorization of the record company. "A great many of consumers were at risk every day," due to the delay, Felten said. "Our exemption request is fundamentally asking for protection for those consumers." Previously, security researchers would notify vendors directly upon finding a flaw, though since the DMCA took effect, the climate has become tainted by fear of litigation, and some security researchers have actually left the field, Felten said. He claims that once he discovered the Sony vulnerability, he contacted his lawyers and opted not to publish his results immediately. Others have argued that Felten would not have had any legal liability had he published his findings, and S. Metalitz of the International Intellectual Property Alliance, an organization representing major copyright holders, has said that Section 1201 already gives security researchers ample latitude to conduct their work. Sony's first attempt at an uninstaller for the rootkit was severely flawed, and Felten and other security experts developed alternatives to better protect against inadvertent reinstallation, though he says that they still fear litigation. Rules against circumventing copyright technologies create risk, said Matthew Schruers of the Computer and Communications Industry Association. "So that raises for me a perplexing question: Why on earth are we putting cybersecurity in the hands of copyright lawyers?"