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

Δελτίο 42
30 Σεπτέμβρη 2006

Technology Lobbyist Named Top US Cyber-Security Official
Washington Post (09/19/06) P. A6; B. Krebs

Greg Garcia has been named assistant secretary for cyber security and telecommunications by the Dept. of Homeland Security, which finally filled the vacancy after 14 months. Garcia, who works at the Information Technology Association of America, will monitor DHS' cyber-security plans for keeping critical information networks secure. DHS chose Garcia after previous candidates for the job were criticized for lack of experience and not having enough power in Washington. President Bush and his administration have been criticized for their slow response to attacks and for not being prepared. Part of Garcia's job includes creating a response plan in the event of a major cyber attack and developing a blueprint for protecting the countries critical information networks, including water and power systems, transportation and telecommunications.

Personalization in Privacy-Aware Highly Dynamic Systems
Com. of the ACM (09/06), Vol. 49, No. 9, P. 32; S. Sackmann; J. Strucker; R. Accorsi

Retailers can personalize their relationship with customers via highly dynamic information systems (HDS), but this can come at the cost of customers' anonymity, write S. Sackmann, J. Strucker and R. Accorsi of the University of Freiburg's Department of Telematics. Users' desire to control personal data is undercut by the exploitation of technologies such as sensor networks, radio frequency identification (RFID), localization technology, and automatic video surveillance in HDS. More and more in HDS, data is being accumulated without any indication, and such collection occurs without any predefined purpose. In addition, the falling cost of data storage means that data remains persistent and undeleted once collected, while customers can be recognized and identified by integrating simultaneous recordings of an event by different devices from multiple perspectives. Furthermore, multiple events are registered concurrently by recording devices. Modern privacy-enhancing technologies are thwartted by the inherent data collection in HDS because of their reliance on obscurity, or the concealment of data, the authors maintain. Sackmann, Strucker, and Accorsi present a proposal for a system in which the transparency of privacy is supported by the creation of evidence, which relies on policies as reference for a compliant utilization of data and log views that cover all data concerning an individual contained in an information system. The proposal ensures the genuineness of log data via secure logging through the employment of standard cryptographic methods, while views on logged data are also a necessity, albeit one that has not yet been provided but perhaps could be through the intercession of regulatory institutions.

Q&A: Go Back to Paper Ballots, says e-Voting Expert
Computerworld (09/20/06), M. Songini

Johns Hopkins University computer science professor and Maryland elections judge A. Rubin heavily criticizes e-voting in his new book, "Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting." He complains in his book that the United States acted without thinking when it instigated the transition to e-voting, which is fraught with

transparency and security problems. Rubin calls for a system that is transparent to average voters and that allows recounts to be monitored as they happen, which requires a paper trail. He does not think a voter verifiable paper trail (VVPAT) is a cure-all to e-voting's problems, explaining that the paper trail "keeps track on a roll in the order of how people voted, but it's impossible to recount because it's so unwieldy. It's still vulnerable to software problems, and if you don't check carefully you can get away with stuff not found in random checking requirements." The irony of the poor voting system in the model democracy is not lost on Rubin, who recommends the jettisoning of electronic polling books in favor of voter registration cards that the voter puts in an envelope taped to the voting machine. "If we can put something in place [for voting] in the next seven weeks, we should," he concludes.

Electronic Voting Machines Are Making Officials Wary
New York Times (09/24/06) P. A19; I. Urbina

An increasing number of state and local officials are growing concerned about the reliability of electronic voting machines as the November elections approach. The most recent warning about the technology came from Maryland Gov. B. Ehrlich (R), who suggested that the state return to paper balloting. Some election officials are concerned that the electronic systems that have been widely adopted since the 2000 presidential election simply trade in old problems for new ones. Roughly one-third of the nation's precincts are using e-voting systems for the first time, boosting the chances of Election-Day problems as poll workers adjust to the new technology. "I think there is good reason for concern headed into the midterm elections," said former Ohio Governor R. Celeste, adding that the new technology creates new demands for training a generation of non-technologically inclined poll workers. The major source of concern has been paperless touch-screen systems, which are expected to be used by roughly 40% of voters this year, raising the prospect of fraud or computer failure. The number of challenges to an election filed in court increased from 197 in 2000 to 361 last year, according to R. Hasen, a professor at Loyola Law School in Los Angeles. Last month, a Pennsylvania state senator introduced a bill to require all precincts in that state to provide voters with the option of using paper ballots, a provision that has already been implemented in at least 27 states. The recent primaries in Maryland, where Election Day problems echoed earlier issues in Texas, Illinois, and other states, were just the latest example of the problems that can go wrong with e-voting systems.

With Homeland Security Grant, Cornell Seeks to Sort Facts >From Opinions
Cornell News (09/18/06); B. Steele

Researchers from Cornell University, the University of Pittsburgh, and the University of Utah have launched a project seeking to train computers to scan text and make a determination as to whether its contents are fact or fiction. The Dept. of Homeland Security created the consortium of three universities as one of four that are exploring sophisticated techniques for information analysis and security-related computational technologies. "Lots of work has been done on extracting factual information--the who, what, where, when," said Cornell computer science professor C. Cardie. "We're interested in seeing how we would extract information about opinions." The research aims to bridge the gap between the distinctly human form of intuitive intelligence and the more literal machine intelligence by giving meaning to sentences through novel machine-learning algorithms. Cardie says his team is also working to rate the sources of a work that a writer might cite. "We're making sure that any information is tagged with confidence. If it's low confidence, it's not useful information," he said.

Researchers Reveal Potential 'Click Fraud'
Indiana Daily Student (09/22/06); K. Oloffson

"Click fraud" could pose a considerable threat to online advertisers because it can go unnoticed, according to researchers at the University of Indiana. In fact, M. Jakobsson, an associate professor of informatics, and research assistants and computer science graduate students J. Ratkiewicz and M. Gandhi are unsure if online attackers have already taken advantage of Web advertisers in such a manner. Online advertisers pay Web sites when Web surfers click on their ads, and scam artists can exploit the business model by having friends visit the site and click on the ads, according to the researchers in a new study. In addition to the social approach, online attackers can employ a technical strategy using "badvertisements," in which tiny ads are placed all over a site, giving the impression that visitors are viewing them. "It's going to be invisible to the advertisement provider," says Jakobsson, who is also an associate director at the IU Center for Applied Cybersecurity Research. "They won't realize there's click fraud on your site." Small pay-per-click advertisers appear to be more vulnerable to click fraud. The researchers will present their study at the Anti-Phishing Working Group's annual conference in November.

Artificial Intelligentsia
Atlantic Monthly (10/06) Vol. 298, No. 3, P. 146; J. Fallows

Debate is brewing over whether the Internet is nurturing a form of artificial intelligence through the group efforts of bloggers, editors, and other Internet users, whose individual pursuits are collectively creating a vast, impartial, and multidisciplinary knowledge base. Atlantic Monthly correspondent J. Fallows expects two significant achievements--spot knowledge retrieval via the embedding of computing power in everyday objects and machine-created categorization--to have an ultimately beneficial effect on human beings' cognitive capabilities. With spot recall, people will be able to retrieve any piece of information whenever they wish, while categorization will give them a leg up in recognizing patterns in the data. Fallows writes that these capabilities will be a mental version of eyeglasses, enhancing the lives of people whose memory fades as they get older. "For those without such problems, these new tools could, while perhaps less immediately essential, yet become the modern-day equivalent of the steam engine or the plow--tools that free people from routine chores and give them more time to think, dream, and live," the author concludes. At the same time, Fallows acknowledges sympathy with technology essayist J. Lanier, who warned in the online publication Edge that collective intelligence would have an effect similar to political collectivism in its stifling of innovation and creativity.

ACM Security Experts to Urge Paper Trails for Electronic Voting
ACM (09/27/06); V. Gold

B. Simons, an electronic voting expert and past president of ACM, will testify tomorrow that voter verified paper trails provide a significant step toward mitigating the risks and ensuring the public’s trust in the nation’s election process. At a Congressional hearing reviewing security for e-voting machines, Simons will cite a range of defenses against multiple security risks, including the kinds of human error that have recently plagued primary elections in several parts of the country. Also testifying will be E. Felten, Professor of Computer Science and Public Affairs at Princeton University. Two weeks ago, his research team released a detailed analysis of the security of one of the most widely used e-voting machines. The US House of Representatives Committee on House Administration will hold the hearing, which will be available via Webcast from 10 a.m. to 12 p.m. EST. Dr. Simons says there is a con-

sensus among computer scientists that all computerized voting systems currently available carry risks. She will recommend that the widely used paperless Direct Recording electronic (DRE) devices produce a voter verified paper audit trail (VVPAT) or voter verified paper ballot (VVPB) to mitigate these risks, and restore transparency to elections. Moreover, she will urge the adoption of policies and procedures that guarantee the integrity of the paper and the quality of the printers used for printed paper trails as well as open, transparent, mandatory manual recount if the manual count does not match the count produced by an e-voting machine.

Vote Check-in Glitch Is Declared Fixed
Baltimore Sun (09/26/06) P. 1A; M. Harris, A. Green

Diebold Election Systems says a flaw in software customized for the state of Maryland was the source of the problem with check-in computers during primary elections earlier this month. The computer glitch caused delays for voters at precincts. Speaking at the state's election office on Monday, T. Feehan, project manager in Maryland for Diebold, said it was "an oversight" that the company did not sufficiently test the software for its e-poll book. Diebold is scheduled to conduct a day-long test of the software for check-in computers next week. The machines also experienced two less-widespread problems during the primary election that Diebold has yet to fix. Feehan said a small number of poll books had communication problems, which would have enabled a voter to cast another ballot at a different poll book in a precinct. Diebold plans to provide a solution for this problem to the state before the end of the week. Moreover, Feehan said some of the voter access cards used to activate voting machines did not work. All of the fixes need to be installed on the state's 5,500 e-poll machines before the general election on November 7. State elections administrator L. Lamone says that if Diebold can't prove that the machines are ready to go, she'll "pack them up and ship them back.".

Johns Hopkins Joins Effort to Boost 'Smart Tag' Security
Johns Hopkins Gazette (09/25/06) Vol. 36, No. 4, P. Sneiderman

Researchers from Johns Hopkins University, the University of Massachusetts Amherst, and RSA Laboratories are collaborating on a project to improve the security of smart tags. Some of the same features that make these devices easy and convenient to use are also potential security threats, researchers say, claiming that thieves can swipe sensitive information from the tags without the user even knowing. The security of smart tags is of increasing importance as the devices are being deployed for applications such as merchant payments and gaining access to medical records. At Johns Hopkins, assistant research professor in the Department of Computer Science A. Stubblefield will use his portion of the NSF grant money to examine the protocol and architecture of the systems, which include RFID tags. "We want to make it tougher for unauthorized readers to communicate with smart tags, and we want to do a better job of preserving people's privacy," Stubblefield said. RFID tags work by transmitting coded data from a chip through the electromagnetic field of a reader antenna, which some scientists are concerned could enable a tech-savvy thief with the right equipment to swipe data from someone's back pocket or purse. The participants in the project, which has been dubbed the RFID Consortium for Security and Privacy, are also working with the San Francisco Bay Area Rapid Transit District to develop the first open, publicly available software application for exploring RFID privacy and security.