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

Δελτίο 43
7 Οκτώβρη 2006

ACM Security Experts Urge Paper Trails for Electronic Voting
Ascribe Newswire (09/28/06)

Ensuring that the US election process is trustworthy is an important function of voter verified paper trails, stated former ACM President Barbara Simons at a congressional hearing reviewing security for electronic voting systems. Simons, founder of ACM's US Public Policy Committee and co-chair of ACM's study of statewide registered voter databases, testified that all currently available e-voting systems carry risks, such as poor design, lack of thorough testing, limited audit capabilities, and inadequate software engineering. "Technology, if engineered and tested carefully, and if deployed with safeguards against failure, can reduce error rates, provide more accessibility, increase accountability, and strengthen our voting system," she noted, adding that the inclusion of a voter verified paper audit trail (VVPAT) or voter verified paper ballot (VVPB) will improve the security of voting systems and provide for routine audits. Princeton University computer science professor E. Felten, a member of ACM's US Public Policy Committee, urged that extra care must be taken in securing voting systems throughout the election process, and called for better certification for software updates to e-voting machines and increased employment of independent security experts. Simons and Felten concurred that the election and technical communities must collaborate to develop trustworthy computerized voting and electronic registration systems.

Study Shows Internet to Be Resilient Against Terror Attacks
Ohio State Research News (09/28/06)

Ohio State professor Morton O'Kelly is co-author of a new study that concludes that a serious attack on Internet network hubs in the US would not likely collapse the Internet, but may degrade its functioning. "There are so many interconnections within the network that it would be difficult to find enough targets, and the right targets, to do serious damage to Internet reliability nationwide," says O'Kelly. Detailed results have been published in the most recent issue of the Environment and Planning B journal. The study used computer modeling to simulate an attack on major Internet backbone facilities, and assumed not all facilities could be attacked at once. Seattle and Boston have the most diverse number of hubs supporting Internet traffic among cities, and therefore are most resilient, the study concludes. The study, conduced with Ohio State graduate student H. Kim and professor C. Kim, was a follow-up to a 2003 study by O'Kelly that assumed that selected city network nodes would be completely knocked out by accidents or attacks. O'Kelly says that is not a likely scenario since peering agreements between carriers makes it very difficult to shut down an entire network node. O'Kelly says, "There is a rich web of connections in these Internet nodes, and a hit on a single city node or even several of them is not likely to wipe out Internet connectivity."

Alliance Aims to Rethink Network Computing and Communications
Rensselaer News (09/27/06)

Researchers at Rensselaer Polytechnic Institute are pursuing research that defense agencies in the United States and the United Kingdom hope will improve wireless sensor networks in ur-

ban environments. Computer science professor B. Szymanski will head a team that will study how complex sensor data infrastructures manage audio, visual, radar, and chemical sensors. The US Army Research Laboratory and the UK Ministry of Defense want to apply the findings to secure networks of sensors, with hopes of giving coalition forces more flexibility on the battlefield. "We are going to take what we already know about sensor network protocols and infrastructure and think creatively about the future designs," says Szymanski. "With information coming from these different sources, we need to know how to make them collaborate to provide the best information while minimizing the chance that they will be detected." Szymanski's team has received $1.85 million to develop sensor network algorithms, which could also have some civilian applications. The project is part of a larger $138 million initiative over 10 years to reevaluate network computing and communication, involving a consortium that includes the University of Southampton, CUNY, LogicaCMG, and IBM.

Penn State Joins International Effort to Secure Wireless, Sensor Networks
Penn State Live (09/28/06)

The US Army Research Laboratory and the United Kingdom's Ministry of Defense has awarded as much as $135.8 million to the International Technology Alliance in Network and Information Sciences, a consortium comprised of 24 members. The money is designated for research efforts focused on high-tech secure wireless and sensor networks. IBM heads the consortium. Other participants include Klein Associates, Columbia University, Carnegie Mellon University, the University of Maryland, Renssalear Polytechnic Institute, and Penn State's Networking and Security Research Center. The consortium's research efforts will cover secure systems, sensor information processing, and other areas. Penn State computer science and engineering professor T. La Porta, director of Penn State's center, says that research is focused on developing algorithms and protocols for timely data transmission. He adds that the algorithms need to work effectively when addressing the various requirements of multiple missions. He says, "The goal of this work is to create algorithms and protocols that ensure the required information is being delivered to the most important applications and people in time for it to be of use. The algorithms must consider requirements from multiple missions, each with different information needs, importance and timeframes, and dynamically configuring the network to gather, process and deliver the data to maximize the utility of the network. To meet these goals, the area team will define methods for quantifying and representing the 'quality' of information, the requirements and importance of each mission, and algorithms for configuring a sensor network."

New Models to Improve the Reliability of Virtual Organizations
University of Southampton (ECS) (09/29/06), J. Lewis

Researchers at the University of Southampton are working on models that will help improve the reliability and trustworthiness of virtual organizations. Such organizations consist of members who are geographically separated--frequently linked by computer networking--but are able to give the outward appearance of being single unified organizations with an actual physical location. The increasing prevalence of virtual organizations with computerized agents acting on companies' behalf is making it more important to ensure that the computerized agents behave responsibly, said Prof. M. Luck. Luck and his team have been working with Cardiff University, the University of Aberdeen, and British Telecom on a project called Grid-enabled Constraint-Oriented Negotiation in an Open Information Services Environment, or CONOISE-G. "The trustworthiness and reputation of agents are significant issues, especially in the context of virtual organizations in which the agents must rely on each other to ensure

coherent and effective behavior," says Luck, adding that there has been little work in this field thus far. The researchers are working to implement a prototype system that examines trust and reputation, standardizing communication, and policing within the virtual organization.

Garcia Looks to Raise Cybersecurity's Profile
Government Computer News (09/25/06) Vol. 25, No. 29

After a two-year vacancy, G. Garcia has been appointed the new assistant secretary for cybersecurity and telecommunications at the Dept. of Homeland Security (DHS). Garcia will be the first person to ever hold the position and seeks to increase the level of awareness of IT security. Garcia is also the vice president for information security programs at the Information Technology Association of America (ITAA) and has been with the group since 2003. "I think they picked the right guy," says J. Tasker at ITAA. "This is his forte, translating real, hardcore technology into policy." Cyber Security Industry Alliance executive director P. Kurtz also believes that Garcia was a good choice. He says, "Greg is a solid pick for the position. He knows information security issues and has good connections in the private sector. He is also earnest and focused. This combination, with consistent senior support within DHS, will enable DHS to move forward on critical information security issues." DHS National Cyber Security Division director A. Yoran and other former cybersecurity officials, including R. Clarke and H. Schmidt, and emphasized the need for to raise the profile of cybersecurity in the administration.

Software Being Developed to Monitor Opinions of U.S.
New York Times (10/04/06) P. A24; E. Lipton

The Dept. of Homeland Security is funding the development of "sentiment analysis" software by a consortium of major universities that uses natural language processing technology to scan foreign publications for negative views on America and its government. The goal of the three-year, $2.4 million grant is to help DHS locate possible dangers to the US. The software would provide Homeland Security personnel with instant access to an entire article that contains subversive statements. While efforts have always been made to stay abreast of global opinions of our country, this new technology will make the process far more efficient. Cornell University, the University of Pittsburgh, and the University of Utah are working on the research, which is led by J. Kielman, who says it could take several years to get the system in place. He says, "We want to understand the rhetoric that is being published and how intense it is, such as the difference between dislike and excoriate." Kielman noted that they are not monitoring US-based news sources. Currently, the system is being fed hundreds of articles published between 2001 and 2002 from a variety of publications and tested on its ability to discern between similar statements. The task of classifying and ranking opinions expressed about America without error has proven quite challenging, says Cornell computer science professor C. Cardie and University of Pittsburgh computer science professor J. Wiebe. Electronic Privacy Information Center executive director M. Rotenberg calls the research "really chilling," and compares it to the Defense Department's aborted Total Information Awareness project. He says the research "seems far afield from the mission of homeland security."

E-Poll Results Undecided
Baltimore Sun (10/04/06) P. 1B; M. Harris

A mock election, meant to test Maryland's voter check-in computers, was held yesterday at the BWI Airport Marriott. While about 10 glitches did occur, many are confident in the system. State Elections Chief L. Lamone said that she will announce her decision on Thursday as to whether or not the $18 million system will be used in the November general election. Although the e-poll machines are touch-screen, election officials realized that when a mouse was attached and used instead of a finger or a stylus, previous communication issues between the computers were no longer a problem. Such issues plagued the September 12 primaries, and the problem of the machines losing contact with others when the screen is touched has still not been figured out. Diebold Election Systems, the company who makes the voting hardware, assures the state that it could supply all the necessary computer mice for the general election. They also suggested installing new software, as an alternative solution. Potential communications problems between the machines on election day could enable somebody to vote more than once. Using the mice, the test went relatively smoothly, and election officials said the machines saved them from several days of work updating voter records after the election.

Rallies Protest Limits on Digital Copying
Reuters (10/04/06)

In what was dubbed a global "Day Against DRM (digital rights management)," groups of concerned consumers and technologists handed out leaflets during rush hours and lunch breaks yesterday in cities such as Boston, Zurich, Paris, and London, in an effort to raise awareness about the technology that places certain limits on copying music and films. One of the leaflets the protesters handed out featured a silhouette similar to those from Apple Computer's advertising campaign with hands tied together with iPod earpiece cords, symbolizing the limitations of iTunes customers who can play their songs only on iPod music players. "This is not aimed against Apple. We're focusing on iPod because it popularizes that DRM is acceptable," said Peter Brown, executive director the Free Software Foundation. In fact, Apple's DRM software is relatively benign, Brown noted. He added that Amazon Unbox's user license and Windows Media Player 11's user agreement are both incredibly restrictive. "The restrictions demanded by the media companies can get tougher, because the technology companies are now competing to get access to the media," Brown said. Meanwhile, Apple and media companies defended their use of DRM software. They said that a lack of a DRM mechanism would open the door to widespread piracy and would threaten the future of legal online sales of digital content.

Computer Science Professor Argues for a Paper Trail With E-Voting
Washington Post (10/04/06) P. A23; Z. Goldfarb

Johns Hopkins computer scientist A. Rubin argues in his book, "Brave New Ballot," that America's elections are in danger due to their dependency on electronic voting technology. He writes that "democracy has never been more vulnerable," and criticizes election officials because, "despite their total lack of familiarity with cryptology, program verification, and formal risk analysis...election officials don't hesitate to give their opinions on security and reliability of their voting systems." Also under fire is Diebold Election Systems, whose popular voting machines are criticized in a report Rubin wrote three years ago for being poorly designed and not resistant to tampering. In the book, Rubin writes, "Machines must be completely trusted not to fail, not to have been programmed maliciously, and not to have been tampered with." He advocates a paper print out that would allow each voter to be sure that the machine

recorded their vote correctly, and serve as a record should a recount be necessary. Such paper records are currently required in 27 States.