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

Δελτίο 110
27 Μάρτη 2008

Lecturer Criticizes Accuracy of the Voting Process
Oregon Daily Emerald (03/13/08), T. Davis

Former ACM President B. Simons will discuss the policy related to voting machines, security, and the possibility of Internet voting on Thursday at the University of Oregon. "As we've been learning, they're just poorly engineered and tend to break a lot," Simons says of voting machines. E-voting became an interest of Simons around 2000, and in 2001 she helped produce a report on Internet voting as a member of the National Workshop on Internet Voting. "The more I learned, the more appalled I got," Simons says. Advocates of the technology initially saw e-voting machines as a way to make voting more accessible to people with disabilities, and then lawmakers at the federal, state, and local levels were overtaken with a gold rush mentality to purchase and deploy systems that vendors promised would work, she says. Concerns about the security of e-voting machine will lead people to question the results of elections, Simons warns.

Bush Pushes Cybersecurity
USA Today (03/14/08) P. 6A; R. Wolf

Attacks on federal government information systems rose by 152% last year, according to the Dept. of Homeland Security. While the rise can be attributed partly to better reporting methods, officials admit hackers and foreign governments are becoming more successful at breaking into government networks. President Bush announced a 10% increase in cybersecurity spending for the coming fiscal year, bringing total funding to $7.3 billion, a 73% increase since 2004. For DHS Secretary M. Chertoff and members of Congress, the budget boost could not have come soon enough. "There are more bad guys out there," says Sen. T. Carper (D-Del.). The lawmaker chaired a Homeland Security subcommittee hearing recently during which he told attendees that in 31% of breaches, "agencies do not know who took the information or how much information was taken." This is no surprise to the Government Accountability Office, whose separate study found that 20 of 24 major government agencies have inadequate cybersecurity defenses. Meanwhile, the DHS is completing Cyber Storm II, a week-long simulated attack to test the strengths of federal agencies against attacks on communications, information technology, and chemical and transportation systems.

Some Viruses Come Pre-Installed
Associated Press (03/13/08), J. Robertson

A number of electronics products made in Chinese factories have been found to contain viruses that steal passwords, distribute spam, and open up computers to hackers. For instance, digital picture frames sold at Sam's Club contained a previously unknown virus that steals gaming passwords and disables antivirus software, according to security researchers at Computer Associates. Viruses have also been found on digital picture frames sold by Best Buy and Target, as well as on Apple iPods and TomTom navigation equipment. Security experts say the viruses are being loaded during the final stage of production, in which the devices are plugged into a computer and tested to ensure that they work properly. Experts note that the viruses are probably coming from a careless factory employee plugging an infected device into the testing computer, rather than hackers or the factories themselves. Nonetheless, hackers could someday use infected Chinese-made devices as an avenue of attack, security experts say. "We'll probably see a steady increase over time," says Symantec computer researcher Z. Ramzan. "The hackers are still in a bit of a testing period--they're trying to figure out if it's really worth it."

Researchers Create Next-Generation Software to Identify Complex Cyber Network Attacks, George Mason University (03/17/08), J. Edgerly

Researchers at George Mason University's Center for Secure Information Systems have developed CAULDRON, software that can prevent successful cyber attacks by identifying possible vulnerabilities in an organization's network. To protect an organization's networks, it is necessary to understand not only individual system vulnerabilities, but their interdependencies. "Currently, network administrators must rely on labor-intensive processes for tracking network configurations and vulnerabilities, which requires a great deal of expertise and is error prone because of the complexity, volume, and frequent changes in security data and network configurations," says university professor and center director S. Jajodia. "This new software is an automated tool that can analyze and visualize vulnerabilities and attack paths, encouraging 'what-if analysis.'" CAULDRON allows for the transformation of raw security data into roadmaps that allow users to prepare for attacks, manage vulnerabilities, and have real-time situational awareness. CAULDRON can show all possible attack paths into a network, can provide informed risk analysis, and can analyze vulnerability dependencies. Jajodia says the software is applicable to almost any organization with a network and resources that need protecting. The Federal Aviation Administration recently installed CAULDRON in their Cyber Security Incident Response Center, helping them prioritize security problems, reveal unseen attack paths, and protect large numbers of attack paths.

Voting-Machine Maker to Princeton Researcher: 'Hands Off'
Wall Street Journal (03/18/08), J. Kronholz

Sequoia Voting Systems has sent an email message to Princeton professor E. Felten suggesting that the voting equipment maker would pursue legal action against him if he were to test the security of its e-voting machines. The Constitutional Officers Association of New Jersey asked Felten to review Sequoia's equipment because it had concerns about malfunctions involving about 60 voting machines during the state's Feb. 5 primary. However, Felten said he received an email on Friday that said Sequoia had "retained counsel to stop any infringement of our intellectual properties, including any noncompliant analysis." The email also says the New Jersey counties would violate licensing agreements if they share their machines with Felten for testing. In a statement, Sequoia says customers have an opportunity to compare the codes of products with those it submits to the National Software Reference Library, and that Colorado, California, and the city of Chicago recently completed independent reviews of its equipment. However, it "does not support any and all unauthorized activities that violate or circumvent our produce licensing agreements," the statement said.

Voting for More Than Just Either-Or
MIT News (03/14/08), D. Chandler

MIT researchers are developing Selectricity, software that could make ranking systems as easy to use as traditional voting systems, creating results that would satisfy a greater portion of the population. Selectricity has been available online as a free service since last fall and is about to switch to an upgraded version with more advanced options. Using Selectricity, anyone can go to the Web site and set up a "Quickvote" in just a few seconds, and users anywhere can access the poll and vote, creating instant results. There is also an ultra-simple version that uses text messaging for voting by cell phones. Although the software is being used for simple tasks such as deciding where to go to dinner or when to hold a meeting, it is sophisticated enough to handle real elections. In February, a beta version of the upgraded software was used by a national student organization to elect their first board of directors, with each of the 16 campus chapters of the Students for Free Culture group receiving an equal vote to select five members for their governing board from a field of 13 candidates. In the election, the candidate that received the most first-place votes, also received the most last- or near-last-place votes, meaning in a traditional election the candidate would have won despite being unpopular with the majority of the voters.

The Future of Voting IT
Government Computer News (03/10/08), W. Jackson

Information technology is the latest trend in voting technology, and could even allow people to vote over the Internet from their homes. However, the debate over how technologically advanced we want our voting systems to be has yet to be settled. Many want to return to a more simplified voting system with mandatory paper audit trails. Advocates of paper trails say that touch-screen systems have not been proven secure. Supporters of electronic voting say that paper ballots have not been proven secure either, and that adding paper ballots to electronic systems adds another layer of complexity. As for whether we will ever feel comfortable voting entirely online, experts are still largely unsure. University of Ottawa PhD student A. Essa, who helped demonstrate a system that makes optical-scan voting more transparent, says that whether or not we like the idea of Internet voting, we should still be doing our best to developed the best online voting systems. University of Waterloo PhD student Jeremy Clark, who also participated in the demonstration at a recent forum on new voting technology, says studies show that online voting actually decreases voter participation because engaging in civic responsibilities is more likely when the process is visible.

Plan to Use Paper Ballots in November Is Reversed in Colorado
New York Times (03/21/08) P. A14; K., Johnson

Colorado lawmakers have scrapped a plan to use only paper ballots in Colorado's November election, which was announced in January as part of a bipartisan effort to replace the state's troubled electronic-voting machines. Opponents of the plan say it was no longer needed because the e-voting machines have been repaired. Supporters of the effort say that questions remain regarding the reliability and security of e-voting and vote-counting machines, and could become a problem again before November. The debate over e-voting in Colorado began in December, when Colorado secretary of state M. Coffman announced that the voting machines used throughout the state failed tests conducted by his office. The idea of using paper ballots faced strong opposition immediately, particularly from county clerks who said the logistics of doing a one-year transformation were insurmountable. Lawmakers recently said the need for a change had been negated by passing a system for expedited retesting and recertification of the voting and vote-counting machinery. A spokesman for Coffman says the new system resulted in all of the machines being recertified in recent weeks. Still, some lawmakers say the recertification process does not address the fundamental problems that e-voting machines are prone to.

Outsider to Run Cyber-Security Initiative
Wall Street Journal (03/20/08) P. A8; S. Gorman

Silicon Valley businessman R. Beckstrom was picked to oversee the National Cyber Security Center, a new agency created by a classified presidential order in January that is part of a covert government initiative to protect government and private computer networks. The center will be based at the Homeland Security Department and Beckstrom will report directly to Secretary M. Chertoff. Officials say the agency will look for ways to protect government networks from terrorists and spies and then use that approach for the private industry. Beckstrom's main task will be coordinating government-wide cybersecurity efforts and generating momentum for an estimated seven-year, $30 billion plan that Bush administration members want to continue into the next presidential administration. National Intelligence director M. McConnell is pushing the initiative to protect networks holding military secrets and due to increasing fears that the US's Internet infrastructure is ripe for attack. Former White House cybersecurity official R. Cressey says Beckstrom will provide a fresh approach to the problem. "Rod's greatest asset is that he's not one of the usual suspects," Cressey says. However, others say Beckstrom's outsider status could be problematic.

After Threats, NJ Clerks Call for E-Voting Investigation
IDG News Service (03/20/08), R. McMillan

The Constitutional Officers Association of New Jersey (COANJ), representing the state's county clerks, has asked the state's attorney general to investigate voting discrepancies observed in e-voting machines used during February's presidential primary elections. "We want to know what the problems were and how do we fix them," says COANJ President M. Dressler. Clerks from six New Jersey counties reported discrepancies in the voting tallies generated by about 60 of the state's Sequoia Voting Systems AVC Advantage e-voting machines during the election. In most cases, the discrepancy involved a one- to two-vote difference between the paper tape logged by the machine and the number of votes stored in the computer's memory cartridges. Sequoia blamed the discrepancy on poll worker error and says the problem can be fixed with a software update, but state clerks have asked for a third-party investigation. COANJ recently asked Princeton professor E. Felten to examine the Sequoia machines, but the plan was abandoned after Sequoia threatened legal action against Felten and the county that offered to provide the systems. Sequoia has since commissioned two independent analyses of the AVC Advantage machines, and the results are expected to be delivered within the next few weeks to Sequoia and to the New Jersey attorney general's office.

Defending Laptops from Zombie Attacks
Technology Review (03/21/08), K. Greene

Laptop-based security software that adjusts to how an individual utilizes the Internet so that the detection of malicious activity is more dynamic and personalized has been developed by Intel researchers. The software targets corporations that pass out laptops and mobile devices to workers, since IT departments typically install homogeneous security software on all their hardware, which partly explains why security breaches are so profuse, according to Intel Research Berkeley researcher N. Taft. Most IT departments deploy security software with a component that analyzes the stream of Internet traffic flowing into and out of a computer, and that suggests infection when traffic exceeds a preset limit. However, this method can incorrectly target people who habitually send out large volumes of information while ignoring traffic that falls below the threshold that may harbor malevolent activity without the sender's knowledge. Intel researchers have devised algorithms capable of more subtle evaluations, including one that creates individualized traffic thresholds by monitoring a person's Internet use through standard statistical and machine-learning techniques, and another that assesses how people's Internet usage changes throughout the day. Another set of algorithms uses the same behavioral principles to study communication between laptops and other devices on the Internet to detect the presence of botnets. "I think the basic takeaway is, if you can be really precise in capturing user behavior, you can make the work of the attackers much harder," notes Taft. Georgia Institute of Technology professor N. Feamster attributes the lack of application of the behavioral security strategy to laptops to the absence of an automated way to develop personalized rules.

Terror on the Internet: A Complex Issue, and Getting Harder
IEEE Distributed Systems Online (03/08) Vol. 9, No. 3, G. Goth

Attempts to crack down on online terror face the challenge of doing so without restricting free speech and access to information, and politicians the world over regularly call for the removal of terrorist sites from their hosts' site servers or for the blockage of access to such sites by search engines. "Those who think that we can stop online terrorism by removal of Web sites are either naive or ignorant about cyberspace and its limitations for interference," says Haifa University professor G. Weimann. "As a short answer, there is a need for strategy and not tactics, there is a need for a multi-measured approach, and not just 'Let's kill those Web sites.'" Weimann says multilateral agreement on fighting Web terror is lacking because the issue is riddled with legal ambiguities, such as who ultimately has authority over the determination of terrorist sites. In addition, there is great disagreement over to what degree content--such as instructions on an arborists' site for making explosives to blow up tree stumps--could be defined as terror-inducing material. Meanwhile, ISPs' efforts to develop filtering and blocking technologies for Web sites owned by a wide range of malevolent parties are being met by jihadists' improvement of work-around strategies. Government-directed anti-cyberterror initiatives include collaboration with independent groups that collect and examine global terror site content, and the development of deep analytic technologies such as Web spiders that can study links between jihadi sites, messages, and forum postings to create white-hat viruses and malware designed to hamstring or compromise jihadi sites.

E-Voting Vendor's Web Site Hacked
IDG News Service (03/20/08) Montalbano, Elizabeth; R. McMillan

Sequoia Voting Systems' e-voting Web site has been hacked, stirring uproar from New Jersey officials that used the Ballot Blog in a February presidential primary. Princeton University computer science professor E. Felten reported the breach, following an inquiry from a state county clerks coalition to investigate the e-voting system. Evidence of the infiltration was apparent because the hacker had inserted a message with a cyber tag name. The system was temporarily suspended and users were redirected to a hosting-provider page, but Sequoia later brought the blog back online. "My guess is that they took the site down temporarily while they were clearing out the stuff left behind by the intruder," Felten says. The county clerks have asked New Jersey attorney general A. Milgram to probe Sequoia Voting Systems AVC Advantage e-voting machines, due to discrepancies in vote counts during the primary. Sequoia says different vote totals were due to poll worker mistakes and warned Felten against investigating it further.