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

Δελτίο 103
24 Γενάρη 2008

Could Post-Ballot Audits Renew Faith in U.S. Elections?
Computerworld (01/16/08), T. Weiss

Observers wonder whether ballots can be efficiently tallied while restoring Americans' confidence in the electoral process even as distrust of electronic voting mounts. A ray of hope may be offered in random, mandatory audits of cast ballots, and support for the concept may be growing. New Jersey Gov. J. Gorzine (D) just passed a law mandating random audits starting later this year, and this statute will dovetail with the state's voter verifiable paper records law requiring electronic touch-screen voting machines to use a paper printout so voters can be certain that their votes were recorded correctly. Coordinator of the Electronic Privacy Information Center's National Committee for Voting Integrity L. Coney says her group advocates mandatory random audits, provided they are truly random. "No one should be able to know where the audits are going to be held [on specific machines]," she argues, adding that the proper performance of a random audit involves pulling the machines from the warehouse, auditing them, and then submitting a report without any early notification on what machines will be audited. Officials can then study the paper ballots and the tallies on the optical scanning machines to determine whether the audit lines up within an extremely thin degree of error to guarantee that the election was completed accurately. Such a strategy eliminates the likelihood that the results of an election can be changed by large enough error, according to Iowa e-voting activist J. Depew. "Every state should be required to do post-election audits to be sure the machines are counting properly, and then if there are discrepancies, they can be going to a hand count" for an accurate vote tally, says VotersUnite.org executive director J. Gideon.

Who Invented the Firewall?
Dark Reading (01/15/08), K. Higgins

Numerous computer experts can lay claim to inventing the firewall. N. Zuk says he developed the technology that is used in all firewalls, and D. Pensak claims to have built the first commercially successful firewall. W. Cheswick and S. Bellovin wrote a book on firewalls in 1994 at AT&T Bell labs and built a circuit-level gateway and developed packet-filtering technology, though they do not claim to have invented the firewall. M. Ranum says his reputation as inventor of the firewall is just a marketing trick and that D. Presotto deserves the credit. Regardless, all of these security experts, along with J. Mogul, P. Vixie, B. Reid, F. Avolio, B. Chapman, and others were associated with the development of firewall technology. Gartner's J. Pescatore says Cheswick and Bellovin were the fathers of the network firewall concepts, using packet filtering to deny everything except what is explicitly allowed, while Ranum was the father of DEC SEAL, the first firewall product. Today, some of the firewall's creators are no longer big supporters of the technology. Cheswick, a lead member of the technical staff at AT&T Research, says he has not personally used a firewall since the 1990s. "They are an economic solution to weak host security. I want to see stronger host security," says Cheswick, who adds that firewalls still have a place but are simply another network element. S. Bellovin agrees. "The firewall as Bill and I described it in 1994 in our book is obsolete," says Bellovin, now a professor of computer science at Columbia University. He

says having a guard at the front door when there are thousands of backdoors into a network does not work. "I'm not saying get rid of it at the door. It provides a low-grade access control for low-value resources," Bellovin says. "But the real access control [should be] at the host."

Voters Respond Favorably to Touch Screen Voting Equipment
University of Michigan News Service (01/14/08), J. Wadley

New research by the University of Michigan, the University of Maryland, and the University of Rochester indicates that voters have more confidence that paperless, touch-screen systems will record their vote accurately, and that voters focus more on what affects their voting experience than on potential fraud, the opposite of what is valued by many computer scientists, voting activists, and a growing number of election administration officials. "Casting a ballot may seem simple, but the interactions between voters and voting system interfaces are complex," says University of Michigan professor M. Traugott. "The more effort involved in voting, the less satisfied voters are with the experience." The study of voting technology examined six voting systems, including paper ballot/optical scan, manual advance touch screen, auto advance touch screen with paper, dial and buttons machine, a full-face membrane with buttons, and a zoomable touch screen prototype not available to the public. The study included responses from 1,540 voters who cast ballots on each machine. Paper ballots and standard touch screens are more accurate when people are casting multiple votes for the same race, however, paper ballots do not work well when the voter needs to change a vote or write in a candidate. "We observed that voters can get quite lost in the voting process and when they do, the chances are greater they will not recover, ultimately voting for no one or a candidate other than they intended," says University of Michigan professor F. Conrad.

Q&A: Ohio Secretary of State Looks Anew at E-Voting
Computerworld (01/14/08), B. Friedman

In the "Evaluation & Validation of Election-Related Equipment, Standards & Testing" (EVERST) report, Ohio Secretary of State J. Brunner made several suggestions to Ohio Governor T. Strickland and state legislators, including eliminating direct-recording electronic (DRE) touch-screen machines and switching to a centralized ballot counting system. During a recent interview Brunner detailed various findings of the report and described some of the report's results, including potential weaknesses with optical-scan units. Brunner says that several independent, parallel tests were conducted, including tests by academic researchers and corporate scientists, and that the independent tests generated similar and sometimes identical results. Eventually, Brunner believes that voters should use a decentralized counting system, but because e-voting security is currently so weak, a centralized system should be used. Brunner says that a major problem with optical-scan machines is the ability to turn off the scanner's memory, which would cause the machine to continue to scan ballots but not record the votes. "Still, if you were to take the report and assign the numbers of risk to each component in the system, I think you're going to see that the greatest number of risks are with the DRE systems," Brunner says. Brunner says her biggest goal is restoring and ensuring voter confidence.

USACM Fears Increased Risk to Identity Theft From Implementation Rules for National ID Plan, AScribe Newswire (01/16/08)

ACM's US Public Policy Committee (USACM) released a statement highlighting flaws in the final standards issued by the US Dept. of Homeland Security restricting how state driver's

licenses and ID cards are provided. The standards were issued as part of the requirements of the 2005 REAL ID Act with the intention of making it more difficult to fraudulently obtain a driver's license. USACM says the standards will not meet the stated purpose of providing a "gold standard" for identification. Additionally, the new standards call for obtaining personal information and sensitive documents that will need to be stored in a form that makes it easier to copy and falsify for fraudulent purposes. "The emphasis placed on the use of REAL ID will provide greater incentives to obtain fraudulent IDs that will then be accepted as 'proof' of identity nationwide," says USACM chair and Purdue University professor of computer science E. Spafford. USACM strongly supports effort to increase security against criminal activity, but Spafford disputes the idea that standardized driver's licenses or identity cards would accomplish such a goal. "Identity should not be confused with intent," he says. "Simply because people's names are known does not prevent them from engaging in criminal behavior or terrorist activities."

Penn State Researchers Help Identify Weaknesses in Ohio Voting Machines
Penn State Live (01/15/08), C. Chan

The report on Ohio's electronic voting machines was recently released by Ohio Secretary of State J. Brunner. The report showed exploitable weaknesses in the state's touch-screen and optical-scan devices. Penn State researchers led by computer science professor P. McDaniel served as a subcontractor to SysTest during the company's testing of Ohio's electronic-voting machines. McDaniel says the research teams, which also included teams from the University of Pennsylvania and the University of California at Santa Barbara, had access to the voting machines as well as the source code from the vendors. Penn State researchers conducted hackability testing and source code analysis, including an examination of recent software upgrades, on the Hart and Premier Election voting systems. "Our report is an extensive technical analysis of the security of these voting machines as they would be used under real-world conditions," McDaniel says. "Our review concludes that the vendor systems lack basic technical protections necessary to guarantee a trustworthy election."

Weak Control System Security Threatens US
Government Computer News (01/16/08), J. Jackson

The weak security measures in place on infrastructure control systems may someday put US utilities at risk of a coordinated attack, says J. Dixon, the former acting director of the Homeland Security Department's National Cyber Security Division. Of particular concern to Dixon are the control systems to utility company substations. These systems are typically controlled by dial-in modems and often have outdated or nonexistent security and authentication technologies. Meanwhile, some of the control systems of utility company substations that are on a network are vulnerable to a crossover attack because they may be sharing their equipment with other, less-sensitive systems. In addition, relatively little logging goes on with control systems, which makes it difficult to determine whether a failure is the result of an attack or misconfiguration. Meanwhile, in research work conducted last fall, the Energy Department's Idaho National Laboratory demonstrated how a megawatt generator could be broken into from a remote location by calling into the substation system and executing a number of malicious commands to change the workflow logic of the generator. In addition to the right phone number to dial into, such an attack would require expertise in electrical engineering and network security. Dixon says the US has been lucky so far, but warns that if the bad guys get organized "we'd have some serious challenges."

Touch Screen Voting a Hit; Critics Miss Mark on Security, Study Says
University of Maryland (01/22/08)

The University of Maryland, the University of Michigan, and the University of Rochester conducted a five-year study concluding that e-voting products, particularly touch-screen voting systems, score highly in terms of voter satisfaction and confidence, but still suffer from key usability concerns that the addition of paper trails cannot redress. Unintentionally failing to cast a vote in some races or voting for the wrong candidate are among the errors that the e-voting systems were susceptible to, and the study recommended necessary improvements to enhance e-voting's user-friendliness, and educational campaigns to guarantee that voters and poll workers are aware of what they are doing. "One of the things we've learned in this study is that training may be even more important than which voting system is used," notes University of Rochester political scientist R. Niemi. Voter verification system tests were carried out separately, and determined that voter accuracy is modestly improved by the devices. The study ascertained an overall voter accuracy rate of 97%, which fell to 80% to 90% as the job of voting became more complex. "Recent history is clear: The election problem most likely to tilt a close race is not security, but the inability of voters to cast their ballots the way they intended," says P. Herrnson, director of the University of Maryland's Center for American Politics and Citizenship. For manufacturers, the study recommended that usability engineering should be stressed at the outset of product development, while voters should be provided with clear feedback on their place in the voting process, review screens should show full information on one screen, the completion of the voting process should be clearly indicated, and systems should not supply too much information at once.

SC Voting Machines Prompt Calls for Federal Action
Cybercast News Service (01/22/08), M. Bansal

Problems with electronic voting machines in Horry County, S.C., during the Republican primaries on Jan. 19 have led to renewed calls for a paper trail requirement. "Voters are understandably outraged that in this important primary election they could not exercise their right to vote because of the machine malfunctions," says Common Cause President B. Edgar. "This was a preventable and foreseeable crisis. Congress and state election officials must move fast to fix this problem by the general election in November." The South Carolina Election Commission blamed the problem on human error while the machines were being prepared. "South Carolina's voting system has performed today as it was designed to perform," the commission said. Election Systems and Software, manufacturer of the iVotronic voting machines used in Horry County, defended the malfunctioning machines. "The iVotronic's three independent but redundant memory paths ensure that no votes will ever be lost or altered," the company says. "Also, if an election is ever contested, iVotronic's unique, patented recount system allows replication of the entire election process, including production of all ballot images for re-verification." Rep. R. Holt (D-N.J.) has introduced legislation that would provide $500 million in federal funding to jurisdictions that convert to paper-based voting systems in 2008, as well as to those that do not fully convert but provide emergency paper ballots. "Voters should never have to leave their polling places wondering if their legitimate vote will be counted," Holt says.

Researcher 'Cracks' Yahoo Anti-Scam Feature
Techworld (01/18/08), M. Broersma

A Russian security researcher claims to have created an automated access system that can bypass Yahoo's CAPTCHA (Completely Automated Public Turing test to tell Computers and

Humans Apart) image-recognition system. CAPTCHAs are used to prevent automated systems from registering Web-based email accounts, filling comment sections with spam, and guessing passwords. Various automated CAPTCHA-cracking systems have been developed, mostly by spammers, but until recently Yahoo's CAPTCHA was ranked as one of the toughest to break. The researcher says his system can attain an accuracy rate of about 35%, and that Yahoo has been notified about the problem but has not responded. "It's not necessary to achieve a high degree of accuracy when designing automated recognition software," the researcher wrote. "An accuracy of 15% is enough when attacker is able to run 100,000 tries per day." Yahoo released a statement saying it is aware of attempts being made toward automated solutions for CAPTCHA images, and it is developing improvements to the system and other defenses.

Cyber Espionage Seen as Growing Threat to Business, Government
Network World (01/17/08), E. Messmer

The SANS Institute has ranked cyber espionage as this year's third-biggest security threat, behind Web site attacks that take advantage of browser vulnerabilities and botnets such as Storm. "Economic espionage will be increasingly common as nation states use cyber theft of data to gain economic advantage in multinational deals," SANS said. "The attack of choice involves targeted spear phishing with attachments, using well-researched social engineering methods to make the victim believe that an attachment comes from a trusted source." Several organizations have been the target of cyber espionage in the last several months. For example, the US Dept. of Energy's Oak Ridge National Laboratory (ORNL) last month acknowledged that about 12 of its staff members received emails urging them to go to phishing sites or open attachments laced with malware. The attack, which some security researchers say was launched in China, was part of a "coordinated attempt to gain access to computer networks at numerous laboratories and other institutions across the country," says ORNL Director T. Mason. China has denied any involvement in the attack. Despite such attacks, the RSA Conference Advisory Board's T. Mather says concerns about cyber espionage are overblown. He believes open source intelligence gathering is a growing industry, with several companies available for hire to scour the Internet for desired information.

IP Addresses Are Personal Data, EU Regulator Says
Associated Press (01/22/08), A. White

Internet protocol addresses are personal information, according to the head of the European Union's data privacy regulators. German data-protection commissioner P. Scharr told the European Parliament that if an Internet user is identified by an IP address, then it must be considered personal data. This view differs from Google, which argues that an IP address identifies the location of a computer, not the identity of the user. Many people consistently use the same computer, which generates the same IP address, a factor that has resulted in the creation of many "Whois" Web sites. These sites allow users to find out the person or company who is linked to a certain IP address. If the EU decides to mandate that IP addresses be considered personal information, it would change the way search engines record data. Google stores search data for up to 18 months, taking the last two numbers off of the stored IP address. This makes the address part of a geographic group, instead of a representation of an individual user. Google stores user's search information in an effort to improve its regional search results and to prove to advertisers that they are not being deceived by "click fraud." Microsoft does not store user IP addresses, instead hoping that users will log into the Passport network that is featured on Hotmail and Windows Live Messenger. A. P. Lombarte, Spain's data protection

regulator, criticized both companies for not clearly stating their privacy policies on their home pages.

Student Develops Anti-Spam Program
Stanford Daily (01/16/08), A. Sy

Stanford University graduate student D. Erickson and computer science professor N. McKeown have developed Default Off Email (DOEmail), a free anti-spam tool that enables users to broadly categorize received mail. DOEmail divides mail into three basic groups--a list of people you want mail from, a list of people you do not want mail from, and an unknown group for all uncategorized addresses. Email received and classified as "unknown" generates an auto-response from DOEmail, which emails a form to the sender to verify that they are a person and not a spam machine. The sender is then given three weeks to respond. Erickson says DOEmail can help users regain control of their inboxes by allowing users to micromanage their spam control or to simply set broad filters and let the program do the rest. He says DOEmail is more effective and more user-friendly than other anti-spam tools such as those based on content filtering. Currently, the 35 users participating in the research project have not received any spam since using DOEmail, which has a plug-in for Mozilla Thunderbird and is accessible to anyone who wants to use it.