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

Δελτίο 46
30 Οκτώβρη 2006

Building a Better Voting Machine
Wired News (10/18/06), K. Zetter

Wired News consulted UC Berkeley's D. Wagner and Princeton's E. Felton in order to come up with a wish list for the ideal voting machine. The two computer scientists agreed that regarding the hardware used, a ballot marking machine is the best option. This device uses a touch screen interface that is universally useable, but instead of recording the votes onto a memory card, it prints votes onto a full-size paper ballot one at a time, rather than off a ream of paper. The ballots are then scanned by an optical reader, which digitally records each vote. The current removable memory cards must be done away with. Security measures are insufficient to assure no tampering occurs. Wagner is researching possible ways to store votes on a memory card so they cannot be changed once entered. As for the software, most voting machines were built for other purposes and converted. The result is code that is excessive and provides camouflage for malicious code. Wagner says the goal is to reduce the code to a minimum. Another problem with the code is that it is kept secret; judges have defended this right of the manufacturers. In order to ensure the integrity of an election, the code must be disclosed. Also needed are machines that can display the programs running on them and recognize if one does not match the approved program. Diebold itself was found to have installed a non-certified version of voting software onto machines in California. Mandatory audits are suggested as well: random spot checks of machines on election day, followed by post-election hand audits to ensure recording and counting is done correctly. The problem of post-election voter verification, however, is not easily solved. Cryptographer D. Chaum is devising a system whereby voters would receive encrypted receipts that could be compared to results posted online after the election. While voting security can never quite be perfected, Felten says all we can do is take steps to "reduce the window of vulnerability."

IU Study: More Internet Users May Be Taking 'Phishing' Bait Than Thought
Indiana University (10/12/06)

A new study from researchers at the University of Indiana indicates that as much as 14% of Americans may be getting duped into giving up private information in "phishing" scams. The figure is much higher than the 3% of adults a year cited in several surveys by Gartner Group. Researchers from IU's School of Informatics settled on 14% after simulating phishing attacks, in which they sent emails with a link to eBay customers that appeared to be legitimate. When recipients clicked on the link, they were sent to the eBay site, and the researchers were notified of the log-in. The researchers also launched a simulated spear phishing attack, in which personal information available online is used to create a more personal message for targets. "We think spear phishing attacks will become more prevalent as phishers are more able to harvest publicly available information to personalize each attack," says J. Ratkiewicz, a computer science doctoral student. M. Jakobsson, associate director of the IU Center for Applied Cybersecurity Research, says, "Our goal was to determine the success rates of different types of phishing attacks, not only the types used today, but those that don't yet occur in the wild, too." "Designing Ethical Phishing Experiments: A Study of eBay Query Features" is the title of the study.

Officials Probe Possible Theft of Voting Software in MD
Washington Post (10/20/06) P. B1; C. Barr

A former Maryland legislator this week received three disks that contain voting software developed by Diebold Election Systems, although what version and how secure the files are is debated. The disks were delivered anonymously to the office of C. Kagan, with an unsigned letter that referred to the disks as "right from SBE (State Board of Elections)" and "accidentally picked up." The theft is being looked into by the FBI, although both Diebold and the State Board of Elections claim that they never had such disks. Diebold's M. Radke says no software on the disks is used in Maryland, but the version of one program on the disks remains in use in "a limited number of jurisdictions," and is properly encrypted. The two programs, for which the disks are labeled as "source code," are: Ballot Station, the operation that controls the touch-screen voting machines, and Global Election Management System (GEMS), which is used in the process of tabulating votes after an election. A. Rubin, a computer scientist at John Hopkins University, as well as an election expert who is very skeptical of e-voting, was given a copy of the disks to research, on the condition he would not make copies. Of the disks' content, he said, "I would be stunned if it's not real." A graduate student at John Hopkins working with Rubin, S. Small, claimed that the version of Ballot Station on the disks "was consistent with what we've seen previously." He was unable to gain access to the GEMS software, however, because two of the disks were protected by a password. Radke points out that new security features have been implemented on versions released since those on the disks, and "it would take years for a knowledgeable scientist" just to get past the encryption on the disks sent to Kagan. However, Rubin says that on the disks he reviewed, "the data and files were not encrypted."

New Laws and Machines May Spell Voting Woes
New York Times (10/19/06) P. A1; I. Urbina

As the election date nears, officials nationwide are preparing for a potentially turbulent day that will test various elements of the election system. Fears range from databases not includeing registered voters, to machines that provide no paper verification, to poll workers who are inadequately trained. Some officials and vendors of voting machines have gone to colleges to recruit computer science graduate students or even posted listings on Monster.com in an attempt to make sure adequate technicians are in place on election day to help see that everything runs smoothly. The combination of new machines and people who are unfamiliar with them worries many. W. Noren, the top election official for Boone County, Mo., is behind in both delivery of machines and staff training. About half of the 45 most highly contested elections will use machines that provide no paper verification, which does nothing to help feelings of uneasiness. D. Markowitz, president of the National Association of Secretaries of State, thinks that since this is not a presidential election and many voters are being encouraged to mail in their votes, that problems will be kept to a minimum, although the worry exists that many legitimate voters will be turned away due to database inconsistencies, which persist after four years of struggling to correct them. Wake County, NC, which uses optical scan machines, experienced technical failures in this year's primaries, but at least those machines provide a paper ballot that can still be counted. Hotlines fielding problems and providing information to voters received about 200,000 calls in 2004, reporting over 40,000 problems. C. Stewart, head of the political science department at MIT, has published a study claiming that from 2000-4, the number of improperly marked ballots was reduced by about one million.

Many echo his feeling that voting problems always occur, and in this time of new technology they are simply highlighted to a greater degree.

Picking Out Digital Image Forgeries
Network World (10/17/06), M. Kabay

M. C. Johnson has developed tools that can help forensic analysts detect digital image forgeries. On October 6, Johnson gave a presentation entitled "Lighting and Optical Tools for Digital Image Forensics." The three techniques he described were illumination direction, specularity, and chromatic aberration. Illumination direction analyzes light sources in a photograph, using a mathematical approach devised by Johnson. The system can calculate the angle of incident light based on the shadows in a picture and recognize any inconsistencies. This software has been successfully built and tested. The specularity tool he is working on looks at reflective highlights in images. The example used to display this system was a picture from "American Idol," in which two contestants had been digitally imposed. He showed that the reflective parts of the photo, such as the eyes, revealed a single light source in the eyes of some people pictured and two light sources in others. The algorithm and program are still in the works for this technology. Finally, chromatic aberration uses the principles of a camera lens and Snell's law. The tool examines the natural distortion of a picture caused by a camera lens. If this distortion is not consistent throughout, then the image is most likely forged. Johnson is still perfecting this technology. While none of these tools is 100% effective on its own, when the three are used in concert with forensic analysis they contribute a great deal to investigations and verifications of forged images.

W3C Launches Secure Browsing Initiative
Business Wire (10/17/06)

The success of the Workshop on Usability and Transparency of Web Authentication has led the W3C (World Wide Web Consortium) to charter the Web Security Context Working Group, a new initiative to devise standards for browsers in an effort to help people decide whether a site is trustworthy. The March workshop, which drew many big technology and online finance companies as participants, showed W3C that there is considerable interest in secure interfaces. W3C expects to attract browser vendors, security experts, research institutes, financial institutions, and end users to the group. W3C says the group will also work with organizations such as IETF, OASIS, and Liberty Alliance. M. H. Zurko of IBM will head the group, which will focus on the information browsers need to provide in order to describe the security context, presenting the information and raising awareness, and improving browsers so they are able to guard against being spoofed. "When I'm browsing the Web, I want my browser to help me understand who really is the owner of a Web page," says T. Berners-Lee, director of W3C. "There is much deployed and proven security technology, but we now need to connect it all the way through to the Web user."

Analysis: 'Total Information' Lives Again
United Press International (10/26/06), S. Waterman

A computer system is being developed by the Office of the Director for National Intelligence J. Negroponte that is capable of mining great amounts of information in order to watch for terrorist planning--technology that recalls the Total Information Awareness (TIA) program. The new effort, known as Tangram, was discovered last week and has been criticized by advocates for privacy and civil liberties. "They are misdirecting resources toward this kind of fanciful, science-fiction project while neglecting the basics" of effective counterterrorism investigation, says T. Sparapani, legislative council with the ACLU. The system is funded for $49 million in research over the next four years, and will build on earlier efforts to create "methods of...effectively searching large data stores for evidence of known [terrorist] behaviors." While intelligence officials insist that the program is within the law, similarities to TIA, which data-mined stores of information including credit-card purchases, telephone calls, and travel records, remain. Congress had cut all funding to TIA in 2003 after substantial concern arose over privacy and civil liberties implications. The Advanced Research and Development Activity, which oversaw the TIA, is also in charge of Tangram. "The administration has flat-out ignored Congress," says Sparapani. "They renamed it, retied the bow and off they went." Three contracts totaling almost $12 million have been awarded for Tangram research and development. Recipients include Booz Allen Hamilton and 21st century Technologies, both of which worked on the TIA project, and SRI International, which worked on a predecessor to TIA, known as the Genoa project.

Internet Voting Revisited
VoteTrustUSA (10/25/06), B. Simons; A. Rubin; D. Jefferson

"Internet Voting Revisited: Security and Identity Theft Risks of the DoD's Interim Voting Assistance System," a new report from four academic computer scientists, details serious security issues with a new absentee-voting system for US military personnel called the Interim Voting Assistance System (IVAS). Created by the Federal Voting Assistance Program (FVAP), IVAS is designed to help military personnel and overseas civilians register and vote in the November 7 election, but the researchers say it has similar security issues to an earlier FVAP program known as SERVE that caused that system to be scrapped. The researchers, including former ACM President Barbara Simons, note that IVAS was publicly announced just last month and has never been used in a public election or primary. The Defense Department's own internal review of IVAS also raised security questions. The DoD's internal review noted that "the transmission of voting materials by unsecured email is a concern from both a privacy and security concern...it is easily monitored, blocked, and subject to tampering." While the report admits encryption is possible, it says "there is no plan" to do so. Transmissions sent over foreign phone systems cannot be secured; the U.S. has enough trouble securing its own telecommunications. The report evaluated two IVAS voting options. Option one: the voter logs into the system and submits information before a ballot is mailed to them, and they mail it back to the DoD. Option two: after logging in and submitting their information, the voter logs onto a server where the ballot can be downloaded, printed out, filled in, and sent back to the DoD. The report says that IVAS opens up voters to potential identity theft, returning ballots electronically allows hackers an opportunity to tamper, and the ballots are handled by DoD, an unnecessary step that places the ballots in possession of the voter's employer, which can be seen as a conflict of interest. The researchers suggest making sure ballots are only sent by mail, and adequately securing the system for requesting ballots via the Internet. Barbara Simons was also co-chair of a USACM committee that studied "Statewide Databases of Registered Voters."

NIST to Certify Voting Machine Security, Standards
eWeek (10/26/06), W. Rash

The US National Institute of Standards and Technology (NIST) will aid the federal Election Assistance Commission (EAC) in its efforts to verify that electronic voting machines meet federal standards. NIST will assist the EAC in creating standards that vendors of e-voting machines must comply with, as they submit their products for testing with private laboratories. "NIST will address security and wireless access," says Brian Hancock, director of voting systems certification for the EAC. Other standards exist such as for usability, performance, and accessibility, and NIST will also focus on these areas as well. Hancock says the EAC wants NIST to concentrate on developing tests, which will be carried out by private labs, that are transparent. Meanwhile, Ian Piper, a representative of the Election Technology Council of the Information Technology Association of America, who is also director of compliance for vendor Diebold Election Systems, says the EAC needs to make testing standards more consistent and stop changing requirements all the time. Over a third of US voters will cast their ballots on e-voting machines this year, says EAC Chairman P. DeGregorio.