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

Δελτίο 133
31 Οκτώβρη 2008

Thousands Face Mix-Ups in Voter Registrations
Washington Post (10/18/08) P. A1; M. Flaherty

New state voter registration systems across the US are incorrectly rejecting voters and threatening to disrupt the election process. The problems are occurring in states that switched from locally managed lists of voters to statewide databases, a change required by the Help America Vote Act. Although the switch is supposed to be a more efficient and accurate way to keep lists up to date, the transition is causing the systems to question the registrations of thousands of voters when discrepancies occur between their registration information and other official records. In Alabama, for example, dozens of voters are being labeled as convicted felons due to incorrect lists, and Michigan is scrambling to restore thousands of names it illegally removed from voter rolls due to residency questions. In Wisconsin, tens of thousands of voters could be affected, as officials admit that their database is wrong one out of every five times it flags a voter, often due to data discrepancies such as a middle initial or a typo in a birth date. Herbert Lin, who is studying the issue for the federal Election Assistance Commission, says that states are not using the "best scientific knowledge known today," as required by law. One of the problems with Wisconsin's database, which has been in place since August, is that 95,000 voters are incorrectly listed as being 108 years old. If no birth date was available when names were moved into the electronic system, it automatically assigned Jan. 1, 1900. By federal law, anyone whose name is flagged must be notified and given a chance to prove his or her eligibility, but voting rights experts say voters are not always alerted, and some, even if they are notified, may simply decide to skip the election as a result.

ACM Experts See Opportunities and Risks for E-Voting
AScribe Newswire (10/15/08)

Three experts from ACM's US Public Policy Committee (USACM) will be monitoring the reliability of electronic-voting equipment as the US Election Day approaches. "Several recent electoral experiences have demonstrated that convenience and speed of vote counting are no substitute for accuracy of results and voter confidence that their vote was cast as counted," says USACM chair E. Spafford. "Today's e-voting infrastructure may not be up to the task but tomorrow's could be--if the technology is engineered and tested carefully, and deployed with safeguards against failure." Spafford, director of the Center for Education and Research in Information Assurance and Security at Purdue University, says that USACM has worked at all levels, from Federal boards down to local polling places, to ensure that effective safeguards are in place and used by computer-based systems. He says that voting technologies that employ software-independent verification systems are the key to building voter trust. He also says a physical record is needed to protect against bugs and malicious code, because it will allow voters to verify that their votes have been accurately cast and it will provide an audit trail if necessary. Spafford also recommends that voting systems be independently tested by qualified technical experts. Other ACM experts include former ACM president B. Simons and USACM member H. Hochheiser, professor of Computer Information Sciences at Towson University.

Researchers Expect Hackers to Prey on Cell Phones
Associated Press (10/15/08), J. Robertson

Georgia Tech security researchers say that hackers will likely target cell phones for use in creating botnet armies. They say that as cell phones get more computing power and better Internet connections, hackers will be able to exploit vulnerabilities in mobile-phone operating systems and Web applications. Millions of PCs have already become part of botnets, and owners generally never know. The Georgia Tech researchers say that if cell phones become absorbed into botnets, new types of scams could be created. For example, infected phones could be programmed to call pay-per-minute 900 numbers, or to buy ringtones from companies established by criminals. The researchers say hackers are particularly drawn to cell phones because they are always on, they are always sending and receiving data, and they generally have poor security. "This is the perfect platform (for hackers)," says Georgia Tech professor P. Traynor. "There are some challenges for the adversaries, but we've seen them overcome the challenges in their way before." One challenge for hackers is learning how cellular networks work, which are tightly controlled by cell phone operators.

Users, Enterprises Pay for Poor Privacy Policies, Study Says
Dark Reading (10/07/08), T. Wilson

Complicated and convoluted privacy policies are causing users to make bad decisions online, potentially threatening the practice of self regulation and privacy on the Internet, concludes a new research report from Carnegie Mellon University researchers A. McDonald and L. Cranor. They say that privacy policies are hard to read, are read infrequently, and do not support rational decision making. The study found that users' time cost associated with reading and understanding privacy policies outweighs the benefit of keeping their data safe, and as a result they generally skip the privacy policy when visiting a new Web site. The researchers determined the cost of reading privacy policies by calculating how long it takes to read them and what that time is worth. The researchers used a list of the 75 most popular Web sites and assumed an average reading rate of 250 words per minute to find an average reading time of 10 minutes per policy. To skim a policy took about six minutes. Overall, the study found that an average time of between 16 to 444 hours a year was needed to read all of the privacy policies, and between six to 215 hours to skim those policies. Based on a rate of $4.50 per hour, the study found that reading privacy policies costs users between $71 to almost $7,000 per year, or approximately $365 billion per year for all Internet users in the US. The researchers say if Web-based services are to work under the current regulatory model, enterprises need to find ways of making privacy policies easier to understand.

Increased Retail Security With Smart Items
Fraunhofer Institute (10/08), M. Briele

Fraunhofer IIS researchers are working on a new technical platform to protect goods during the shipping process through the use of wireless ad-hoc sensor networks to create logistical information systems that allow items to be tracked along the entire distribution chain. By fitting small computers with communications facilities into logistical objects, each item becomes an active part of an IT system. The intelligent logistical objects, or smart items, are an advance over passive RFID systems that only transmit their information when requested. The active approach solves fundamental problems in distribution logistics and means. For example, smart items can increase the transparency of shipping goods by making a comprehensive record of all items in a consignment. Smart items also create an active retail surveillance system, because they notice when something is removed from the consignment and can inform the IT system of the loss, not only preventing losses from within the flow of goods but also registering any manipulation or incorrect handling. Fraunhofer researchers are currently working on developing all of the necessary elements, including ad-hoc network mechanisms, network protocols with power-saving media access tiers, efficient routing algorithms, distributed services and middleware, and application-specific software.

Newcastle Scientists Help Microsoft and Yahoo Improve Online Security
Newcastle University (10/21/08)

Newcastle University computer scientists have cracked the Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) security systems used by Microsoft's and Yahoo's email systems, exposing a widespread vulnerability. Both companies believed their systems were secure enough to stop widespread abuse by spammers, but the researchers have demonstrated a method for solving the security puzzles, says professor J. Yan, who will present his findings at the ACM Computer and Communications Security Conference, which takes place October 27-31, in Alexandria, Virginia. Yan says his research shows that computers are able to solve CAPTCHAs with greater ease than previously thought. Using a desktop computer, Yan and PhD student S. El Ahmad used a seven-step method, taking less than 80 milliseconds, to remove the arcs that link letters in CAPTCHAs to make them hard to isolate, and then identified the characters in the right order. The researchers were able to isolate each of the 8 characters more than 90% of the time, and solve the puzzles correctly 60% of the time. The best line of defense, Yan says, appears to be allowing the characters to touch or overlap each other, juxtaposing characters in any direction to make it harder to tell real characters and other "noise" apart, and randomizing the width of the characters.

Keyboard Sniffers to Steal Data
BBC News (10/21/08)

Doctoral students M. Vuagnoux and S. Pasini from the Security and Cryptography Laboratory at the Swiss Ecole Polytechnique Federale de Lausanne (EPFL) were able to monitor what people type by analyzing the electromagnetic signals produced by every keystroke. The EPFL students developed four attacks that will work on a variety of computer keyboards, leading them to declare that keyboards are not safe to transmit sensitive information. Vuagnoux and Pasini tested 11 keyboards that connected to a computer through either a USB or PS/2 socket, though the attacks also work on keyboards embedded in laptops. Each keyboard tested was vulnerable to at least one of the four attacks they developed, with one of the attacks being effective at a distance of 20 meters. The students used a radio antenna to fully or partially recover keystrokes by detecting the electromagnetic radiation emitted when keys are pressed. The research builds on previous work by University of Cambridge computer scientist M. Kuhn, who explored ways of using electromagnetic emanations to eavesdrop and steal useful information.

Beware the Digital Zombies
New York Times (10/21/08) P. B1; J. Markoff

Networks of infected computers that can be used to send spam or launch denial of service attacks, known as botnets, continue to be a growing problem on the Internet. Microsoft's T. Campana recently demonstrated that an unprotected computer running an early version of

Windows XP, and attached to the Internet, can be infected in only 30 sec. In September, more than 500,000 computers were under the control of active zombie networks, according to botnet tracker shadowserver.org. While security experts have managed to reduce the number of machines in botnets to approximately 300,000 computers, that number is still double the number detected a year ago, and the actual number of zombie machines could be even larger. Microsoft's R. Lai says the mean time to infection is less than five minutes. Any computer connected to the Internet is vulnerable, and security experts recommend PC owners run a variety of commercial malware detection programs to find infections, protect their machines behind firewalls, and install security patches for operating systems and applications. Even these precautions are no guarantee. Secunia recently tested a dozen leading PC security suites and found that the best one detected only 64 out of 300 software vulnerabilities that could be exploited to install malware. Botnet attacks even come with their own antivirus software, enabling the programs to take over a computer and remove any other malware competitors. Botnets also are becoming increasingly difficult to detect. Last year, botnets started using a technique called fast-flux, which generates a rapidly changing set of Internet addresses to make the botnet more difficult to locate and disrupt. Companies are now realizing that the only way to fight botnets and other computer crimes is to form a global alliance that crosses corporate and national boundaries.

Rice Students Challenge Electronic Voting Machines
Converge (10/13/08)

As part of an advanced computer science class, Rice University professor D. Wallach is challenging his students to rig a voting machine. Wallach split his class into teams. During phase one, teams pretend to be unscrupulous programmers at a voting machine company by trying to make subtle changes to the machines' software that will alter the election's outcome without being detected by election officials. The second phase has teams playing the part of election software regulators by trying to certify the code submitted by another team during the first phase of the class. "What we've found is that it's very easy to insert subtle changes to the voting machine," Wallach says. "If someone has access and wants to do damage, it's very straightforward to do it." He says the experiment shows how vulnerable certain electronic-voting systems are. Wallach says the students often, but not always, are able to find the hacks, but that in real life it would probably be too late. "In the real world, voting machines' software is much larger and more complex than the Hack-a-Vote machine we use in class," Wallach says. "We have little reason to believe that the certification and testing process used on genuine voting machines would be able to catch the kind of malice that our students do in class."

National Cybersecurity Initiative R&D Effort Launched
Federal Computer Week (10/14/08), B. Bain

The National Science Foundation has issued a request for information (RFI), launching the National Cyber Leap Year, which was established to seek the most promising ideas for reducing vulnerabilities to cyberactivities by altering the cybersecurity landscape. The project seeks to create an integrated national approach to making cyberspace safe for "the American way of life." The project specifically aims to form a national research and development agenda that identifies the most promising technologies and determines how to bring those technologies to fruition. National Cyber Leap Year will run during fiscal 2009. In January, the Bush administration launched the Comprehensive National Cybersecurity Initiative, and while much of the initiative remains classified, officials have released more information on the scope and detail of the multiyear effort in recent months. NSF is seeking leap-ahead research and technology to reduce vulnerabilities due to asymmetric attacks in cyberspace. "Unlike many research agenda that aim for steady progress in the advancement of science, the leap-ahead effort seeks just a few revolutionary ideas with the potential to reshape the landscape," the RFI states. The first stage of the Leap Year project involves surveying the cybersecurity community for ideas. The second phase will involve a series of workshops to develop the best ideas.

A Really Secret Ballot
Economist (10/22/08)

The security of elections should be bolstered by the encryption of ballot papers, which is the goal of the Pret a Voter process developed by P. Ryan at Britain's University of Newcastle upon Tyne. In the process, paper ballots are scanned by an optical printer, and the ballots are halved, with candidates' names on one side and tick boxes on the other. A voter selects the desired tick box and divides the paper, placing only the half with the tick on it in the ballot box. The candidates are arranged in random order on each ballot paper, making it impossible for anyone looking at the deposited half of the paper to know which candidate was selected, but not impossible for the machine to know thanks to a cryptographic cipher containing the candidate order. The Scratch & Vote approach devised by B. Adida and R. Rivest of the MIT utilizes a ballot paper that is similar to the one used in Pret a Voter, but extra security is added with a scratch-off area containing the data used to randomize the candidate order on that particular paper. The data can decrypt the individual cipher on the ballot when combined with a public key, which is distinct from the private key used by election officials to unlock the vote in the absence of the original randomization data. Computer scientist D. Chaum's Scantegrity II approach involves the voter marking his candidate choice by filling in a bubble with special ink that reacts with a pattern of two chemicals printed within the bubble. One chemical darkens the entire bubble so that a standard optical reader can record its position and the chosen candidate, while the other chemical becomes visible in a contrasting hue to uncover a previously invisible three-character code derived from a pseudorandom number generator. This code is unreadable by the vote-counting machine, but the voter can note it on a detachable receipt at the bottom of the ballot paper and then check the correctness of the vote by entering the serial number of his ballot paper into an election Web site to see if the letter code matches.

Photo Safeguards Confidential Information
University of Twente (10/27/08)

A University of Twente student has created a technique for protecting photographs stored on mobile phones. I. Buhan, who recently received her doctorate from the Faculty of Electrical Engineering, Mathematics and Computer Science, uses a photo of the face of the user of the mobile device to create a biometric record, relying on a mathematical method to store the facial recognition data securely. Her system is capable of recognizing the user even if she has changed their hair style. Buhan went a step further in also making the system capable of securely transferring photos from the device owner to another mobile phone user. Her approach is to construct a password from two photos by having two users save their own photos on their PDA, then take photos of each other and have the device compare the two photos and generate a security code for a safe connection. Photos are exchanged using this connection, and the photos are stored as a template that contains the key features for recognition. Other biometric recognition systems would be able to apply this safe template transfer.

Princeton Report Rips N.J. E-Voting Machines as Easily Hackable
Computerworld (10/27/08), T. Weiss

Electronic-voting machines used in New Jersey and elsewhere are unreliable and potentially prone to hacking, concludes a new report from Princeton University and other groups. The 158-page report was ordered by a New Jersey judge as part of an ongoing dispute over the machines. The e-voting machines can be "easily hacked" in about seven minutes by anyone with basic computer knowledge, according to the report. The vulnerability could enable fraudulent firmware to steal votes from one candidate and give them to another. The machines can be hacked by installing fraudulent software contained in a replacement chip that can be installed on the main circuit board, which would be very difficult to detect, the report says. The major problem is that there are numerous opportunities in the storage, distribution, and deployment of the machines where an unauthorized person could access and manipulate them without being detected. Princeton University A. Appel, one of the authors of the report, says that such vulnerabilities cast doubts about the accuracy and reliability of the machines. A group of public interest organizations are plaintiffs in a lawsuit against the state of New Jersey, arguing that the machines should be discarded because they cannot meet state election law requirements for security and accuracy. State officials who support the machines say they are adequate for the job.

ACM Experts Say Heavy Voter Turnout Will Test New Voter Registration Systems
AScribe Newswire (10/28/08)

The 2008 US election will test many newly installed or redesigned voter registration databases (VRD), warn ACM computing experts. The 2002 Federal Help America Vote Act required states to establish the databases, but they have become a source of confusion in early voting currently underway in several states. Experts from ACM's US Public Policy Committee (USACM) will monitor and analyze the reliability of registration records and voting equipment around the US as the election approaches. Federal law requires states to verify new voter registrations against drivers' license numbers, or the last four digits of Social Security numbers, but the databases containing this information are often flawed. Former ACM president B. Simons says VRD need to control data-entry errors and large-scale data merges and purges, as well as security concerns to prevent voter disenfranchisement, personal information leaks, and voter fraud. ACM's report on VRD includes 99 high-level recommendations to help states establish best practices for computerized statewide electronic databases. Simons says long delays and contested voter eligibility have been caused by problems with VRD systems. USACM chair E. Spafford says that electronic VRD might make registration and voting procedures more efficient, but he is concerned that mismanaged updates could erase thousands of people from voting rolls. Spafford says automated checks should be done well in advance of an election so voters can contest "no match" results.

Good Code, Bad Computations: A Computer Security Gray Area
UCSD News (10/27/08), D. Kane

University of California, San Diego (UCSD) graduate students E. Buchanan and R. Roemer, building on previous research by UCSD professor H. Shacham, have demonstrated that the technique of building malicious programs from good code using return-oriented programming can be automated. They also demonstrated that this vulnerability applies to RISC computer architectures as well as the x86 architecture. Shacham has already described how return-oriented programming could be used to force computers with the x86 architecture to act maliciously without infecting the machines with new code. However, the attack required extensive manual construction and appeared to rely on a unique quirk in the x86 design. Buchanan and Roemer will present their work at ACM's Conference on Communications and Computer Security (CCS), which takes place Oct. 27-31 in Alexandria, Virginia. "Most computer security defenses are based on the notion that preventing the introduction of malicious code is sufficient to protect a computer," says UCSD professor Stefan Savage. "There is a subtle fallacy in the logic, however: simply keeping out bad code is not sufficient to keep out bad computation." Return-oriented programming starts with the attacker taking advantage of a programming error in the target system to overwrite the runtime stack and divert program execution away from the path intended by the system's designers. However, instead of injecting malicious code, this technique enables attackers to create any kind of malicious computation or program using existing code.

New 3-D Image Systems to Provide Reliable Face Biometrics
University of Hertfordshire (10/28/08)

People who wear makeup or wigs will not be able to dupe a new three-dimensional (3D) face-imaging system developed by researchers at the University of Hertfordshire. "Our new 3D vision system goes beyond the skin and is equivalent to measuring the bone structure," says Hertfordshire professor S. Ramalingam. Ramalingam developed new mathematical algorithms for the face-imaging system. Specific segments and features of a person's face can be photographed and then compared with the overall photo. "This is much faster than any 3D system and processes 24 frames per second in real time," Ramalingam says. The face-imaging system can be used in high security zones, and has other commercial applications.