

**Democrats May Give Voting Machines More Scrutiny  
National Journal's Technology Daily (11/14/06), M. Martinez**

Paper trails for e-voting machines may become a reality under the newly-elected Democratic Congress. Concerns continue to be raised about the security of e-voting machines, and the problems uncovered in several races during the recent election gave voting-rights activists no reason to abandon the issue. Rep. R. Holt (D-N.J.) plans to reintroduce in the next session his bill that would mandate e-voting systems leave paper records, and the proposal has attracted more than 200 of his colleagues as co-sponsors. The House got a late start in addressing the issue, as the House Administration Committee did not hold its hearing until late fall. Voting-rights activists are also optimistic because Rep. J. Conyers (D-Mich.), who was a major figure in investigating e-voting problems in Ohio for the 2004 presidential election, is in line to become the next chairman of the House Judiciary Committee. And in the Senate, Sen. D. Feinstein (D-Calif.), who is poised to head the Rules Committee, plans to introduce a companion bill to the House bill that would also require paper records. "It will be a different environment," Holt's spokesman P. Eddington says of Congress.

**Election '08: Vote by TiVo  
Wired News (11/14/06), K. Axline**

While electronic voting has met its share of critics and difficulties, many believe the technology should be worked with rather than completely scrapped. VoteHere founder J. Adler believes that elections could, and should, be made completely electronic, with voting taking place online. He says, "The technology is done. It's really an issue now of politics and people's will." Online elections have been held in Arizona and Michigan, as well as Estonia, Switzerland, Canada, and England; and head of elections for Swindon, England, A. Winchcombe, said the system performed very well, and that "People did try to hack it, but no one got through. The security levels were very high." Those such as Adler believe that any voting system would have inherent flaws, and that it is useless to assume that the technology will fail outright. One way to solve the problem of the vulnerability of home PCs would be a set-top box running open source, verified, and digitally-signed software; voters would be given a receipt containing a serial number by which voters can verify ballot-box results. Several scientists interviewed agreed that this set-top technology would quell many of their e-voting concerns. While it has been shown to increase turnout, the idea of voting from home not only opens up issues of voter confidentiality and coercion, but it makes the assumption that every voter has Internet access. Meanwhile, other experts say online voting suffers from a dependence on inherently insecure home PCs, the threat of denial-of-service attacks, and database hacks. University of California at Berkeley computer science professor D. Wagner says voting "over the Internet is crazy," while computer scientist D. Jefferson says that "there's really no way to secure the transmission of votes over the Internet."

**New Computer Software Enable Rapid Response to Time-Critical Emergencies  
Newswise (11/16/06)**

The US Dept. of Energy's Argonne National Laboratory and University of Chicago researchers presented specialized software at SC06 that allows quick access to supercomputers and distributed computational grids in emergency situations. The system, called Special Priority and Urgent Computing Environment (SPRUCE), "makes massive resources available on short notice for critical applications," including public health, safety, and security emergencies, according to SPRUCE project leader and Argonne National Laboratory computer scientist P. Beckman. The demonstration at SC06 displayed scientists demanding immediate access to the TeraGrid of supercomputers at the University of Chicago in order to execute analyses of a developing weather emergency in which time was of the essence. Resources connected to SPRUCE are able to preempt current functions for emergency response, or execute the emergency computations immediately after a current function is finished. "Severe weather predictions can be computationally intensive and naturally the workload is unpredictable," says NSF Linked Environments for Atmospheric Discovery and University of Oklahoma associate vice president for research K. Droegemeier. Beckman's vision of the future of emergency response is that "all of the nation's supercomputers will be ready to provide urgent computing to support and protect the nation."

### **Exterminating the Nuisance of Spam CNet (11/15/06), D. McCullagh**

The United Nations Internet summit in Athens, Greece, earlier in November was beneficial because it brought NGOs, regulators, law enforcement, and ISPs together and enabled the various stakeholders to share their ideas on how to curb spam, according to S. Ramasubramanian in an interview with CNet. Ramasubramanian, the head of antispam operations for Outblaze, says convincing more email users not to click on attachments, persuading ISPs to get involved in anti-spam mailing lists, and getting regulators and NGOs to pass anti-spam laws would be a big help in reducing spam. He is also an advocate for capacity-building for people, training sysadmins, promoting open source, and improving connectivity. Developing countries have become the source for a large percentage of spam, says Ramasubramanian. Outblaze filters messages for sites such as Lycos, Mail.com, and Register.com, and Ramasubramanian believes the ratio of spam to legitimate email is at least 10 to 1. He adds that a good spammer who launches 1 million messages a day is likely to reach less than a fraction of legitimate email addresses. Spammers' costs remain low by doing a botnet or an open relay, and they are able to make money off of the 2-3% of people who decide to buy their products.

### **Scholars Challenge the Infallibility of Fingerprints Chronicle of Higher Education (11/17/07) Vol. 53, No. 13, P. A14; P. Monaghan**

Scholars' warnings that fingerprint analysis is not faultless are falling on mostly deaf ears, and key to their arguments is a dearth of scientific scrutiny. University of California at Irvine professor S. Cole, author of "Suspect Identities: A History of Fingerprinting and Criminal Identification," points out that because courts have not needed more substantial scientific examination of fingerprint analysis techniques, law-enforcement agencies "retain legal carte blanche to claim that fingerprinting is validated and infallible. They have nothing to gain and everything to lose from validation studies." Cole notes, for example, that examiners use "latent" prints that often do not provide whole, undistorted images, which are then compared to much clearer inked or scanned prints in police databases. The obscuring of myriad details of the print can lead to mistakes. Michigan State University computer science professor A. Jain believes fingerprint technology can only be improved upon, not perfected, and he started a biennial competition to bring such improvements to light. University of Southampton rese-

archer I. Dror thinks fingerprint examiners make mistakes because human cognition is not infallible, and he has run experiments that show that the perceptions and judgments of even expert analysts can be shaped and disrupted by cognitive and psychological effects. Practitioners of fingerprint identification have been nonresponsive to the researchers' findings, and Cole contends that forensic scientists are convinced that the research "doesn't matter because it doesn't hurt them. They operate in the courtroom, where the scholarly literature is just ignored." However, there does appear to be increasing pressure for reform.

### **Attack of the Bots**

**Wired (11/06) Vol. 14, No. 11, P. 171; S. Berinato**

Autonomous software programs or "bots" can coalesce into networks that execute all kinds of mischief on a global level, and this has emerged as the latest threat to the Internet. Bots proliferate like viruses by installing themselves on Net-linked computers; but while viruses follow a rigid program and act individually, bots can be controlled externally from a remote server and work in concert to perpetuate mayhem. Bots can coordinate distributed denial-of-service attacks for the purposes of extortion, distribute spam, facilitate identity theft and credit card fraud by stealing passwords and other sensitive information via keystroke logging, and automate the process of clicking on ads that generate per-click revenue, to name a few strategies. Bots scan for susceptible systems where they can spread, and command and control (C&C) software can upgrade botnets with new abilities as they are devised. Former Arbor Networks researcher J. Linden says, "Bots are at the center of the undernet economy. Almost every major crime problem on the Net can be traced to them." Users usually rent botnets from an intermediary or "bot-herder," whose forte is marketing. Without an effective defense against botnet attacks, the Internet could become increasingly unfriendly to online commerce, or spark more and more severe vigilantism by users, fueling a botnet arms race. The continuing demand for better bots has fueled an intense competition among bot software developers to innovate, and their resulting code attracts a wide array of customers, including organized criminals, political activists, and corporate spies. Meanwhile, Symantec security director V. Weafer testified before Congress last year that 20 nations now have ongoing computer attack programs. Researchers are working on ways to defend against C&C programs, such as alerting ISPs to disable the C&C, but many move too fast, as the bot writers are far ahead technically, says SRA International's A. Meyers.

### **Did Florida Foul Another Ballot?**

**Wired News (11/17/06), K. Zetter**

Critics contend that touch-screen voting machines may have lost over 18,000 votes cast last week in Sarasota, Fla., for a congressional seat, and are calling the recount currently underway a joke because e-voting systems lack a paper trail and questions about the missing votes have not been addressed. A planned legal challenge that will probably be filed next week could help to finally, clearly demonstrate the unreliability of e-voting machines, according to critics. Voters who cast ballots before the election claimed the machines were not recording their selection in the congressional race, and noted that the screen seemed to record their vote when they cast it, but showed no vote cast on the review page. A potential calibration problem with the touch screens was also indicated by reports of vote-switching difficulties. "We're hoping this situation in Sarasota is going to show how absolutely insane it is to have these machines recording our votes...or not recording our votes," declared the Florida Fair Elections Coalition's S. Pynchon. Rep. Rush Holt (D-N.J.) and other lawmakers are using the

Florida debacle as an opportunity to support a bill pending in Congress that would make voter-verified paper trails a requirement for all e-voting systems in the United States.

### **Cracked It!**

**Guardian Unlimited (UK) (11/17/06), S. Boggan**

UK Identity and Passport Security claims that the new passports it is issuing are sufficiently encrypted to prevent fraudulent activity, but some experts have found flaws in the new system. The International Civil Aviation Organization (ICAO) set new standards for passports in 2003 that mandated a RFID microchip included in passports that can only be read with a key consisting of the passport number, the holder's date of birth, and the passport's expiration date, all of which are printed on a "machine readable zone" of the passport; when the passport is swiped by an immigration official, the key is fed into the scanner that is then allowed to read the RFID chip; the passport holder's information is displayed on the official's screen. Bunker Hosting Security technical director A. Laurie explains, "The information in the chip is not encrypted, but to access it you have to start up an encrypted conversation between the reader and the RFID chip in the passport." He was able to write software in 48 hours that allowed him to communicate with the chip; Laurie says that although the Home Office used state of the art encryption technology, it also used non-secret information (actually written in the passport) as a "secure key," a potentially fatal, and foolish, flaw. The Home Office points out that the information that can be extracted from the chip is that which is already on the passport and in order to access it you need visual access to the passport, but German DN-Systems Enterprise Solutions founder L. Grunwald has been able to create a RFID clone that could be used to enter a country illegally, a technique others agree is a dangerous possibility. Pictures on the RFID chip cannot be altered, but simple visual confirmation of a person's appearance has not been proven as an effective security measure.

### **Malware Goes Mobile**

**Scientific American (11/06) Vol. 295, No. 5, P. 70; M. Hypponen**

It was inevitable that increasingly sophisticated mobile phones or smart phones would become susceptible to malware, writes F-Secure chief research officer M. Hypponen. More than 300 kinds of malicious programs that target smart phones, including worms, spyware, and Trojan horses, are at large today. Hypponen says there must be a unified effort by the security community, cellular network operators, smart phone designers, and phone users to check the spread of mobile malware before it reaches epidemic proportions. The decreasing cost and increasing sophistication of smart phones is boosting their popularity to the point where such devices could conceivably comprise most of the world's computers in the near future, and this will offer an irresistible target to malware creators seeking to exploit smart phone users' unfamiliarity with computers and their vulnerabilities. "Carriers would be wise to begin educating cellular customers now about how to identify and avoid mobile viruses, rather than waiting until these infections become epidemic," Hypponen suggests. "Phone makers should install antivirus software by default, just as PC manufacturers now do. And regulators and phone companies can also help avoid the monoculture problem that plagues PCs by encouraging a diverse ecosystem for smart phones in which no single variety of software dominates the market." Hypponen also supports the inclusion of firewalls into phones, and argues that governments should play a more prominent role in addressing the threat of mobile malware.

### **A Conversation With Douglas W. Jones and Peter G. Neumann**

**Queue (11/06) Vol. 4, No. 9, D. Jones; P. Neumann**

Examining the security of electronic voting machines yields insights on the challenges of developing and running trustworthy systems for other applications, and advocates of election process integrity D. Jones and P. Neumann discuss the matter. Jones notes that "any attempt to scientifically investigate elections has unavoidable political implications" regardless of the technologies in use. He says the need for a transparent election system lies at the root of much of the technological difficulties inherent in assuring election integrity. Jones contends that "the entire system must be sufficiently open and comprehensible that non-technical observers can believe the results." Redundancy itself offers no assurance without carefully planned placement and transmission of copies, and clear techniques for spotting and addressing discrepancies between copies; Jones also calls for the support of auditability in voting system design, secure authentication methods to prevent fraud as well as accidental error, trusted ways to transport all system elements, and a way to assess how well the systems fulfill design requirements. Jones observes that while the Help America Vote Act has spurred migration to statewide voter registration databases, the trade-off is statewide ramifications for mismanagement. When asked by Neumann to elaborate on embedding transparency into the electoral process, Jones cites the need to make voting-system failures a matter of routine investigation and to publicize the results of such investigations, as well as ensure that the documentation needed to interpret any public records is also public. As far as using the Internet is concerned, Jones thinks it is a viable option for functions that currently employ wireless systems or other public networks, but he urges more use of satellite voting places for early voting rather than unrestricted postal voting.

### **Electronic Voting Trend May Be Short-Circuiting Sarasota Herald-Tribune (FL) (11/19/06), V. Hull**

An audit of the congressional election in Sarasota County, Fla., is at the center of a push to require electronic voting machines to produce paper records, or to even ditch electronic voting altogether. Support is rising in Congress for legislation requiring a paper trail, and a bill has even been filed that would require a hand count for the presidential election. Twenty-seven states have already passed a paper-trail mandate, some also requiring audits of the electronic voting process. The Sarasota election was mentioned by Democrats in Congress and is seen by many citizens as a clear indictment of e-voting, since there is really no way of figuring out what went wrong, as e-voting expert Avi Rubin of Johns Hopkins University points out. Votersunite.org executive director John Gideon feels that an examination of the Sarasota problem will serve as "a death knell" for the technology. Verifiedvoting.org's David Dill believes optical-scan voting would have prevented the Sarasota problem, while others would only feel comfortable with hand-counted paper ballots; but both of these systems have been found to have their share of flaws as well. Officials such as Charlotte County, Fla., elections supervisor Mac Horton, whose district uses the same machines as Sarasota County, are reluctant to abandon the costly system. "I've been very well pleased," says Horton. "If it's left up to me, I'd stay right where I'm at."

### **Phishing Toolbars: All as Hopeless as One Another Techworld (11/20/06), J. Dunn**

Anti-phishing Web browser toolbars are not very effective, concludes a new study conducted by Carnegie Mellon University researchers and supported by the National Science Foundation and the US Army Research Office. The study, "Finding Phish: An Evaluation of Anti-Phishing Toolbars," looked at 10 browser toolbars to determine their anti-phishing abilities

and concluded that even the most capable toolbars (Earthlink, Google, Cloudmark, MS Internet Explorer 7, and Netcraft) identified only 85% of malicious Web sites, while the rest of the toolbars (eBay, Geotrust's TrustWatch, Stanford University's Spoofguard, Mc Afee's Site Advisor) scored below the 50% mark. "Overall, we found that the anti-phishing toolbars that were examined in this study left a lot to be desired," said the authors of the study. "Many of the toolbars tested were vulnerable to some simple exploits as well." A good deal of those tested delivered a significant amount of false positives, which the researchers viewed as equally harmful because of the lack of trust this could breed in users. The researchers concluded that all filters must be used with care, and that the filter itself, not the browser it is used with, determines the level of security; the ability of the heuristics applied to detect fraudulent sites, and the usability of the software design for the user are the most important aspects of security.

### **Hard-working Chips May Reveal Encryption Keys** **New Scientist (11/20/06), W. Knight**

"Branch prediction" could put the modern microchip at risk to hackers, according to J.-P. Seifert of the Univ. of Haifa in Israel and the University of Innsbruck in Austria, and colleagues. Microchips second guess the logical flow of a program before the actual execution from branch to branch as a way to process information at a faster rate. However, branch prediction can tip off hackers about encryption key details that are processed, if there is a rapid increase in the work it performs and the time required, which would result from a need to perform another operation or a mistake. In a few thousandths of a second, Seifert and his team were able to figure out a high-security 512-bit encryption key, which is often used to protect online financial information and email messages from eavesdroppers. "Security has been sacrificed for the benefit of performance," says Seifert, who suggests the "Simple Branch Prediction Analysis" attack method could be carried out by hiding a small piece of software on a target computer. The researchers have posted their work online, and will participate in the RSA Security conference in February 2007.