

**A Paper Trail for Voting Machines
New York Times (01/07/08) P. A25; W. Poundstone**

A general mistrust of voting systems seems to be a common theme with American voters, as a wave of electronic voting machine de-certifications and negative reports cast doubt over new era voting machines, writes author W. Poundstone. However, paper ballots are also problematic; ballot boxes can be lost or stuffed and it was the paper-ballot/hanging chad fiasco in the 2000 election in Florida that led to the rapid adoption of electronic voting machines. MIT computer scientist R. Rivest and mathematician and voting reform advocate W. Smith have proposed a solution that combines paper ballots and a Web site to create better ballot security than is possible with paper or e-voting alone. The concept is to allow each voter to take home a photocopy of a randomly selected ballot cast by someone else. Paper ballots would be tallied by optical scanners, or even by hand, and results would be posted on a Web site. Using a serial number assigned to each ballot, voters could check the site to make sure that the random ballot they brought home was posted on the site and that it was not altered or misread. Rivest and Smith believe the system creates public accountability as any voter can check to make sure the ballots are being counted correctly, and that only a small number of participant would be needed to catch any fraud. The system also protects voter privacy because the ballots distributed for authentication would be randomized and would not contain voter information.

**German Activist Move to Block E-Voting
Computerworld (01/08/08), J. Kirk**

German computer club the Chaos Computer Club (CCC) has asked a court to grant an injunction that would prohibit the use of electronic voting machines in state elections scheduled for later this month. CCC's F. Rieger says the government does not have the technical knowledge to ensure that machines have not been manipulated. E-voting machines made by Nederlandsche Apparatenfabriek (Nedap), with software from Groenedaal, are currently scheduled for use in an election on Jan. 27 in eight cities and districts in the German state of Hesse. Meanwhile, another e-voting case filed in early 2007 is currently pending before Germany's Constitutional Court, which could influence any future use of e-voting machines in Germany. Nedap machines have been used in the Netherlands, France, and Germany without controversy, but in each country activists tried to stop the use of the machines due to security concerns. In a 2006 paper, Dutch researchers found that undetectable control over the machines and the election could be obtained in a short amount of time, and that radio signals from a Nedap model could be used to eavesdrop and monitor how people vote.

**Fraudsters Beware: Iowa State Engineer Is Developing Cyber Technology to Find You
Iowa State University News Service (12/27/07), M. Krapfl**

Iowa State University professor Yong Guan and his students are developing technologies to fight cyber crime and make online activities more secure. One of the technologies detects "click fraud," in which the number of clicks to ads posted on Web sites is falsely inflated in

order to increase pay-per-click advertising. Guan says the technology will help online advertisers such as Google and Yahoo reduce fraud. Guan also says that his research could help millions of computer users who do not have the time or ability to ensure their machines are updated with the latest security patches and safeguards. Guan is developing technology and techniques for collecting evidence from computers, network hardware, cell phones, and electronic devices to help find the true origins of cyber criminals and attackers. Guan is also working on three projects to improve the security of wireless networks. The first examines how a new secure coding model can be protected from attacks while transmitting network traffic. The new method sends and combines messages in groups to save energy and increase capacity. The second project aims to develop location-based security systems for wireless technology by limiting access to certain documents or networks based on location. The third project will help secure wired and wireless multicasts by protecting and managing lists of Internet accounts, which could help limit access to content.

Malware Honeypots Wait for '08 InfoWorld (12/28/07), M. Hines

The Distributed Open Proxy Honeypot Project, launched by the Web Application Security Consortium (WASC) in January 2007, will be re-introduced with new improvements in January 2008. After collecting data for 11 months, project researchers spent December 2007 reviewing results and strategizing for 2008. As a result, in 2008 WASC will fine-tune its methods for tracking malware distributors and will also expand its existing network of honeypots. The WASC initiative monitors Web traffic for malicious activities using a network of 14 specially-configured open proxy servers. The innovative system is more effective than traditional honeypot applications, which cannot offer sufficient real-time intelligence for defending against modern, swift, customized threats, says WASC project leader R. Barnett. The WASC effort gains new information about cyber-criminals' techniques by advertising its undefended open proxy server to the Internet as the type of anonymous conduit preferred by attackers. System improvements in 2008 will involve implementing more successful methods for correlating anomalies and categorizing attacks. Project researchers would also like to gain assistance from the open-source community in analyzing the raw data. The proxypot model enables researchers to monitor the source IP addresses being utilized by cyber-criminals. Further analysis of the results would let WASC determine which sites were being targeted and notify any companies concerned. At the moment, the project aims to develop an early warning system to facilitate the security industry's response to attacks as they emerge, though the project could one day be used to uncover malware sources and block threats.

Individual Privacy Under Threat in Europe and US, Report Says Associated Press (12/30/07)

International rights group Privacy International warns that individual privacy is under threat in the US and Europe as governments introduce surveillance and information-gathering legislation in the name of security and controlling borders. Privacy International reports that Greece, Romania and Canada have the best privacy records of 47 countries studied, while Malaysia, Russia, and China rank the worst. Britain and the United States are ranked as "endemic surveillance societies," the lowest-performing group. "The general trend is that privacy is being extinguished in country after country," says Privacy International director S. Davies. "Even those countries where we expected ongoing strong privacy protection, like Germany and Canada, are sinking into the mire." In the United States, civil liberties groups have criticized the Bush administration for its involvement in domestic wiretapping, which allows mo-

monitoring of international phone calls and email messages involving people suspected of terrorist links, without a warrant. Britain was criticized for plans for a national identity card, a lack of government accountability, and the world's largest network of surveillance cameras. Davies says the loss of computer disks with personal and bank information on 25 million people in Britain highlights the risk of centralizing information on huge government databases. The report says that privacy protection is generally worsening across Western Europe while it is improving in former Communist states in Eastern Europe. The report also says concern over terrorism, immigration, and border security is driving the spread of identity and fingerprinting systems, often without regard to individual privacy, and that the trends are being fuelled by the development of a "profitable surveillance industry dominated by global IT companies and the creation of numerous international treaties that frequently operate outside judicial or democratic processes."

As Primary Season Ramps Up, an E-Voting Snapshot Computerworld (01/08/09), T. Weiss

There is not enough confidence in electronic touch-screen voting machines to warrant their use by the 450-500,000 voters that are expected to participate in the country's first presidential primary this year, according to New Hampshire deputy secretary of state D. Scanlan. Such devices face major trust issues from voters and election officials, in view of security problems and other woes that have plagued the machines. An EVEREST study on Ohio's e-voting systems was so critical of the devices' security that Ohio Secretary of State J. Brunner instructed all state election officials to supply paper ballots to every voter who requests one as an alternative to touch-screen machines. Optical-scanning machines that read and count votes from paper ballots will collect votes from approximately three-quarters of New Hampshire's voters, while another quarter of the voters will use paper ballots that are counted by hand. "We like to go with something simple and reliable that maintains the confidence of the voters," says Scanlan. Concerns about the security, accuracy, and reliability of touch-screen machines led to the decertification of an array of devices from various vendors for use in California, although some were later recertified under new rules. The new regulations dictate that just one touch-screen machine will be allowed for use in each polling place, specifically for disabled voters.

Open Source Code Contains Security Holes InformationWeek (01/08/08), C. Babcock

Numerous security exposures have been discovered in Samba, the PHP, Perl, and other popular open source projects, according to a review by the Dept. of Homeland Security. Like its commercial equivalent, open source code typically includes one security hole for every 1,000 lines of code. Some projects, such as Samba, have fixed the majority of the vulnerabilities identified by the Homeland Security review. Other projects, such as FreeBSD and Firebird, have been slow to respond to the scans' findings. Overall, roughly 116 of the 180 projects being examined are utilizing the scans and are correcting their security defects. Samba and Linux, along with some other projects, were found to have a substantially lower rate of defects than average, according to D. Maxwell of Coverity, manufacturer of the source code checking system used in the review. Since the review was launched in 2006, a total of 7,826 open source project vulnerabilities have been resolved.

Big Brother Really Is Watching Computerworld (01/14/08), R. Mitchell

The Dept. of Homeland Security is investing in Project Hostile Intent, an initiative whose goal is to detect unfriendlies posing as benevolent parties through the automatic identification and analysis of behavioral and physiological cues affiliated with deception. However, critics contend that the behavioral profiling system's development will take much longer than the DHS is expecting, assuming that it works at all. Current areas of research include recognition of gestures and microfacial expressions, analysis of variations in speech, and grading of physiological characteristics, which the DHS hopes to integrate in order to boost the predictive accuracy rate higher than what other deception detection techniques yield. The accuracy rate of deception detection technologies under development as part of Project Hostile Intent varies according to cultural background and personality type, while lab testing may not necessarily mirror real-world situations. Developers of microexpression recognition technologies complain that they need more psychological data in order to optimize the algorithms that associate expressions with deception, while rules also need to be applied in the proper context. Another project being pursued by DHS' human factors division is an effort to model violent intent via the application of social behavior theory in order to help analysts extract relevant information as they review documents. Privacy advocates are also concerned that Project Hostile Intent's collection of personal data and its risk of generating false positives could be detrimental for innocent people, including racial and ethnic minorities, who are wrongly singled out as suspicious. The behavior profiling systems developed through Project Hostile Intent may eventually be used by the Transportation Security Administration.

New Predictive Approach Seeks to Stay Ahead of Hackers EE Times (01/11/08), S. Riley

Military and academic researchers from the Rochester Institute of Technology, the University of Buffalo, Pennsylvania State University, and the US Air Force are working on CUBRIC, an intrusion prediction project that uses mathematical models and algorithms to predict a hacker's probable moves after having penetrated a network. "We want to be one step ahead of them and predict what they are going to do," says RIT computer engineering professor S. Jay Yang. "When they first get in, we try to observe what they are doing, and use that information to forecast their probable future actions." The goal of CUBRIC is to provide information on how an intruder will react to particular network defenses and architectures so that administrators can lessen damage and better protect their systems. Intrusion prediction modeling is meant to be a part of a larger network protection plan and is designed to defend against the different tactics used by network intruders, such as interrupting service or stealing data. CUBRIC is capable of following individual attackers, or tracking multiple attackers, and will have both commercial and military applications.

South Carolina Officials See No Problems With Touch-Screen Voting Machines Anderson Independent-Mail (SC) (01/12/08), D. Williams

Election officials in Anderson, Oconee, and Pickens South Carolina report that they do not expect to have any problems with the electronic voting machines used in those counties. Officials anticipate a smooth voting process for both the Republican presidential primary on Jan. 19 and the Democratic primary on Jan. 26, and say that tampering with the voting machines is nonexistent. "I would say it would be quite remarkable if anyone did attempt it," says Pickens County Registration and Elections Commission director A. Harris. "There is security in place to prevent tampering, including the poll workers and poll watchers for the candidates and the parties." However, Clemson University computer science professor E. Hare says there are problems with the machines, as shown by the study of Ohio's voting machines,

and that replacing the counties' iVotronics machines with a paper ballot scanned into a computer would ensure a more accurate and verifiable vote count. "Computer scientists have been saying for 10 years that elections are much too important to trust to a computer that you can't verify," Hare says. "It is not enough to trust that the machine tallied the vote accurately. You should also be able to verify that the tally is correct."

Bank Card Attack: Only Martians Are Safe
ZDNet Australia (01/11/08), L. Tung

Security researchers from Cambridge University have discovered a way to attack chip and PIN cards. Cambridge students S. Murdoch and S. Drimer recently demonstrated that the cards do not need to be cloned to be compromised, crippling the banking industry's claim that the cards can only be compromised through card holder error. By tampering with a chip and PIN terminal, Murdoch was able to use a "relay attack" to capture authentication information sent from the merchant's point of sale terminal to the bank. The compromised information can be transmitted over Bluetooth, GPRS, or GSM networks to someone who then uses the information for a fraudulent transaction. Once the information is obtained, the fraudulent transaction must occur within the time that the legitimate cardholder's card is being read by the terminal. Murdoch says he alerted the banks to this possible exploit a few years ago, but that it was dismissed. "The banks general response to this, and, in fact, to everything we do, was that the people from Cambridge are very smart and we find it very amusing but these are lab conditions and it's not going to work in the real world," Murdoch says. Murdoch proposes several adjustments that would make the chip and PIN cards more secure, such as making terminals tamper-resistant, ensuring the numbers embossed on the card match the receipt, and imposing time constraints on the authentication.

Q&A: New Technologies Pose Online Privacy Uncertainties, Rotenberg Claims
Computerworld (01/02/08), P. Thibodeau

In terms of the new perspective on privacy held by Facebook-using young people, Electronic Privacy Information Center executive director M. Rotenberg feels the true privacy issue is that social networking sites covertly gather information to utilize for marketing purposes. In general, Rotenberg asks the question "Are companies being fair with what they do with the data they collect?" to determine whether rules need to be established to protect customer privacy. Privacy law advocates are often simply calling on companies to provide more disclosure about their practices of data collection and use. In terms of RFID tags, Rotenberg explains that many individuals in the privacy and security communities are unhappy about the Dept. of Homeland Security's new "vicinity read" RFID tag standard. Such tags remove the individual's ability to identify when the tag's data is being read, which breaches the principle of basic access control, says Rotenberg. Remote RFID tags could be exploited in many ways; credit card numbers that have not been encrypted, medical data, and information on overseas US travelers could all be pulled by hackers, according to Rotenberg, which is why the e-Passport proposal from the US State Department had to be overhauled. Rotenberg adds that EPIC has been critical of many new proposals from DHS regarding personal identification, border control, and video surveillance. Rotenberg claims many of these proposals, such as the Real ID card, have not been fully thought through, and contain many fundamental security problems. Overall, secure systems of information are those which are only utilized for their premeditated purposes.