The ACM Conference on Computers, Freedom, and Privacy
Technology Review (05/03/07), S. Garfinkel

The annual ACM conference on Computers, Freedom, and Privacy, now in its 17th year, was once the only venue where topics such as cyber-rights, wiretaps, and cryptography policy were discussed. SRI International's P. Neumann, who has been following computer security and related risks for years and is the man who named Unix, opened the conference by saying the problem is that people believe computers are trustworthy and that while we try to boost security systems, the threat truly comes from people who have legitimate access to those systems and intentionally violate their positions. B. Schneier from Counterpane Systems spoke on how the younger generation has a different approach toward security, commonly posting everything in their lives online at social networking sites, even to the extent that some reveal company secrets. W. Diffie, from Sun Microsystems and inventor of public key cryptography, talked about the need for the government to run surveillance so it can know what its citizens need, but that surveillance should be regulated. Diffie pointed out that the 1994 Communications Assistance for Law Enforcement Act, which required all telephone switches to have wire-tapping technology built in and originally excluded the Internet, could now be applied to VoIP as it is being to replace regular phone service. Some of the other speakers touched on subjects including the use of computers in mapping the human genome and rights surrounding the use of genetic information, and problems with organizations, particularly non-profits, losing their domain names to pornographic sites.

Florida Acts to Eliminate Touch-Screen Voting System
New York Times (05/04/07) P. A19; T. Sexton, C. Jordan

Florida state legislators passed a vote to replace touch-screen voting machines in 15 counties as a result of trouble with the machines in the 2000 presidential election. The new system, which is scheduled to be operational in time for the 2008 presidential election, uses optical scan voting machines, which are used in Florida's other 52 counties. The plan was approved by the Florida Senate last week and passed through the House of Representatives unanimously on May 3. In November 2006, more than 18,000 votes cast on touch-screen machines were not recorded in what became a close and highly contested Congressional race in Sarasota County that was won by Republican V. Buchanan by only 369 votes. Florida state officials said the switch to optical scanning is expected to cost $28 million, but the federal Election Assistance Commission said the state could use money from the Help America Vote Act, which provides money to improve voting equipment. Critics say the switch will be more costly than estimated. Palm Beach County election supervisor A. Anderson believes his county alone will cost $19 million. Touch-screen machines can still be used for voters with disabilities until 2012, under the new legislation, but after that paper-ballot technology will be required.

Hacking the Online Ballot Box
Guardian Unlimited (UK) (05/03/07), D. Bradbury

A series of high-tech pilot projects gave some voters in the United Kingdom the opportunity to cast their votes over the Internet in elections on May 3, but experts are questioning the reliability and security of Internet voting. Despite security evaluations by the Department for Constitutional Affairs (DCA) and the Electoral Commission, independent experts identified flaws in a least two of the election's pilot projects, calling them "catastrophically weak" and claiming it would have been easy to manipulate votes in some districts testing the software. The DCA said it was aware of potential loopholes but believes security procedures were strong enough to withstand hacking attempts, and the Electoral Commission said Internet security will be one of the major areas it will examine while reporting on online voting. Even with these reassurances, the e-democracy organization Open Rights Group's voting campaign coordinator J. Kitcat worries that the lack of a paper trail makes oversight difficult and even threatens democracy. Part of Kitcat's fears may stem from problems in the United States with direct recording electronic voting machines (DREs), which became a heavily debated issue in the 2000 election when G. Bush and A. Gore were within a few hundred votes of each other. Talks of vote stealing were widespread, and some states have since banned the heavily scrutinized machines. Former ACM President B. Simons, a computer scientist and Internet voting expert, notes some of the dangers in Internet voting that DREs avoid. "At least you have a chance of doing an audit with a DRE," Simons says. "With Internet voting, you can't." Simons says DRE voting could be made more transparent by designing the machines to print marked ballots based on the voter's entry that could be fed into an optical scanner to register the vote, and provide a paper trail in case of an audit.

Network Warfare
Government Computer News (04/30/07) Vol. 26, No. 9, W. Jackson

The Cyber Defense Exercise is not only the capstone program for information assurance classes at the nations military academies, but is also a rigorous competition that will test the academies' computer science students against a hand-picked group of National Security Agency security experts called the Red Team. Students from West Point, the Air Force Academy, the Naval Academy, the Coast Guard Academy, and the Merchant Marine Academy all participate in the five-day competition where the Red Team will try to break into and shut down a network built by the students. The network is required to include a Web server providing dynamic content from a back-end database, an email server with public encryption, chat service, file sharing, and a Domain Name System for name resolution. To simulate real-world use and the possibility of users exposing the network to malicious programs, the NSA hid malware in a virtual machine that must be included in the network. The students are allowed to search the machine for malware, but the NSA experts are too good at hiding things, according to Air Force Academy assistant professor of computer science Capt. S. Butler. The test starts with the Red Team probing the networks, looking for obvious points of entry, and gradually escalates as the hidden malware sends information back to the Red Team and they eventually begin their full assault on the last day. The score is based on how long the academies can keep their network working, and the winner will receive the coveted NSA Information Assurance Director's Trophy and bragging rights for a year, but the exercise is more than a competition. "Are they fully prepared for it? No," said Coast Guard Academy electrical engineering instructor Lt. J. Benin. "But they learn that what they are learning in class has value."

Florida Ditches Problematic Touch-Screen Voting, and Now What?
CNet (05/04/07), D. McCullagh

Computer scientists attending ACM's Computers, Freedom, and Privacy conference in Montreal on Friday were critical of electronic voting machines. Former ACM President B. Simons participated on a panel with experts who said Florida made a wise decision to eliminate touch-screen voting machines. The computer scientists took particular issue with the fact that many e-voting machines do not have audit trails, which leaves the voting results open to the possibility of manipulation through a software bug or by a malicious attacker. They favored an analog solution in the form of a paper trail. "We are called Luddites," said Simons. "Which I thought was funny coming from people who don't understand technology." Florida lawmakers voted to employ optical-scan balloting instead.

Putting Coders' Security Chops to the Test
Application Development Trends (05/02/07), J. Waters

The SANS Institute will launch a series of assessment and certification exams this summer that are designed to test programmers' security coding skills. The program will consist of four examinations, each covering a different programming language suite: C/C++, Java/J2EE, Perl/PHP, and .NET/ASP. The tests will measure technical proficiency and expertise at identifying and fixing common programming errors that create security vulnerabilities. Anyone interested will be able to test their skills unofficially by taking the tests online, but those who want to receive the GIAC Secure Software Programmer certification must take the exams in a proctored setting. SANS director of research A. Paller says the original plan was to provide an assessment tool but a request from the US Depτ. of Defense convinced the organization to add the certification option to the program. Cigital CTO and security expert G. McGraw says he doubts a multiple-choice test is an effective measure of a programmer's knowledge of software security, but Paller says the SANS Institute's underlying objective is to influence computer science educators. "We hope that, if they see that the security skills of their graduates are going to be measured by their bosses, they will begin to embed this in all of their programming courses," Paller says. "We want to make sure that when you learn to code, you learn it with security baked in."

Web Browsers Are New Frontline in Internet War
New Scientist (05/05/07) Vol. 194, No. 2602, P. 28; J. Hecht

Hackers have found a new way to turn PCs into "zombies" by infecting them with malware via their browser, a loophole that thwarts firewalls and antivirus software. This development reflects a shift in botnet controllers' infection strategies away from email and toward Web sites. At a recent conference on botnets, Google security specialist N. Provos sounded an alarm on "drive-by" downloads of bots from unsuspicious Web sites. Provos' team determined that approximately 450,000 analyzed Web pages launched such downloads of malware, while another 700,000 launched downloads of software that aroused suspicion. Provos explained that users would be unaware of the infection unless their browser began to crash or they were inundated by pop-up advertisements, while Web site owners would not be alerted to the corruption of their Web pages because such malware is usually concealed. Also taking place is a change in the nature of botnets that could make their disablement more difficult, as attackers investigate the potential of peer-to-peer botnets instead of reliance on an Internet relay chat server to transmit instructions. C. Zou of the University of Central Florida in Orlando says users could reduce the likelihood of bots contaminating their PCs while Web surfing by keeping their browsers up to date with the latest software patches.

Document Shell-Code Attacks on the Rise

InfoWorld (05/02/07) Hines, Matt

Targeted attacks that exploit vulnerabilities in popular document file formats--including Microsoft Word, Excel, PowerPoint, and Adobe PDF--and execute via hard-to-find shell code are becoming a growing threat, researchers at IBM's Internet Security Systems division have found. Experts working with the ISS X-Force group said they have noticed a rapid rise in the volume and variety of shell-code execution attacks leveled at their customers over the past year. Customers have been falling for these attacks in large numbers, the ISS division said, due to the fact that the threats typically come from spoofed email addresses that appear trustworthy and reside inside documents that do not have the same security concerns as Web-based applications. Compounding the problem is the fact that most anti-virus applications do not look for shell-code attacks, and intrusion protection systems miss many variants because the types of documents being used are harder to scan for potential threats. Microsoft and Adobe have also been finding it difficult to quickly patch the security vulnerabilities in their products, said X-Force's Kris Lamb. In an effort to correct this problem, Microsoft is working on improving its vulnerability testing process by rethinking some of the heuristics tools it uses to search for potential security vulnerabilities, according to M. Howard, the program manager on the company's security team.