A Dog or a Cat? New Tests to Fool Automated Spammers
New York Times (06/11/07) P. C1; B. Stone

Captchas security puzzles are becoming increasingly easier for programs to solve, and increasingly more difficult for humans. The problem is that as online miscreants create better ways to bypass or defeat captchas, Web companies are responding by developing puzzles that are more difficult to solve, even for people. "They are creating tests that a reasonably healthy adult can't pass," says G. Weakliem, a programmer and blogger who said he failed a captcha test several times on the Microsoft Windows Live sign up page. To create puzzles that will block computers but be easier for people to solve, researchers are focusing on expanding the test beyond the current repertoire of 26 letters and nine digits. Microsoft has developed a captcha that asks Internet users to view nine images of household pets and select just the cats or dogs. "For software, this is wildly hard," says Microsoft research J. Douceur. "Computers are tripped up by all the photos at different angles, with variable lighting conditions and backgrounds and the animals in different positions." The project is called Asirra, short for Animal Species Image Recognition for Restricting Access, and uses graphics of animals from a database of more than 2 million images. Other companies have chosen to keep their captcha projects secret, but PayPal's chief information security officer M. Barrett says that PayPal's new tests may resemble image recognition and present pictures of, for example, a whale, a tree, and a head of lettuce, and ask the users to select the vegetable. "Captchas have gotten as good as they are going to get, and it is likely they are going to be slowly supplanted with a different technology that achieves the same thing," Barrett says.

AU Finds Success With Voting System
Opelika-Auburn News (06/11/07), A. Weaver

The Prime III voting system, developed at Auburn University's S. Ginn College of Engineering, has tested well on three separate occasions and has already impressed some state officials. The machine's designers are confident that it will win at the University Voting System Competition in Portland, Ore., next month, and hope that it will continue to gain support with state and federal legislatures. Associate professor of computer science and software engineering J. Gilbert says the machine is usable by anyone, even if they cannot read, hear, or see, and even if the person has no limbs. Prime III gets its name for its three methods of voting--touch, voice, or both. Instructions are provided through a headset or on a computer screen. Votes are cast by either touching the screen or saying a corresponding number. After testing with students and faculty at Auburn last fall, area senior citizens in February, and students at the Alabama Institute for Deaf and Blind a few weeks ago, the system changed slightly from its original design. Paper ballots were abandoned as a back up system in favor of a video system that records what buttons are pressed and serves as an additional security measure, making it impossible for any hacker that managed to get into the system to go undetected, according to Gilbert. "It is so straightforward for a voter and yet is so complicated for a hacker," Gilbert says. The system's security has not been tested, but Gilbert says that will happen soon.

Antivirus Fix in Works by Security Researchers
Network World (06/07/07)

A new report from researchers at the University of Michigan's Electrical Engineering and Computer Science Department and network security company Arbor Networks offers a solution for improving antivirus technology. In the report, "Automated Classification and Analysis of Internet Malware," the researchers call for a new classification technique that "describes malware behavior in terms of system state charges (e.g., files written, processes created) rather than in sequences or patterns of system calls. To address the sheer volume of malware diversity of its behavior, we provide a method for automatically categorizing these profiles of malware into groups that reflect similar classes of behaviors and demonstrate how behavior-based clustering provides a more direct and effective way of classifying and analyzing Internet malware." Over a span of six months, the approach proved to be useful on 3,700 malware samples. Antivirus products lack some consistency in identifying worm, phishing, and botnet attacks, and some experts have termed the traditional, signature-based approach dead because of the growing virus and malware problem.

Casting Ballot From Abroad Is No Sure Bet
New York Times (06/13/07) P. A1; I. Urbina

The Defense Department has spent more than $30 million over the past six years trying to find a way to help the 5 million American soldiers and civilians living abroad vote securely and efficiently, but no clear solution has been found so far. The Pentagon's current Web-based system is slow and confusing and filled with security and privacy problems, according to security experts and Congressional auditors, who say the system is vulnerable to undetectable hacking and vote tampering. Only 63 voters used it in the 2006 election to request and return ballots via the Internet, according to the Defense Department. Although the department is responsible for helping all overseas voters, civilians are not allowed access to the system. The traditional paper ballots sent to overseas voters have also caused problems, as voters often wait until the last moment to return the ballot, get confused because rules and deadlines vary state to state, and ballots are often lost or delayed in the mail. The end result is that anywhere from a quarter to half of all overseas voters fail in their attempt to vote, according to voting experts at the National Defense Committee and the Overseas Vote Foundation. Military officials say their voting system is merely a means of expanding options beyond the use of regular mail, and that voting assistance officers have been placed in military units worldwide. Department of Defense spokesman S. Upton did not answer questions about the military's system, except to say that the Pentagon has asked for suggestions from the private sector on how to improve the system before the next election.

Purdue Creates Scientifically Based Animation of 9/11 Attack
Purdue University News (06/12/07), S. Tally

An animated simulation of the attacks that toppled the towers of the World Trade Center on Sept. 11, 2001, has been created by Purdue University researchers so that structural engineers can study the buildings' collapse in order that future disasters may be avoided. "Scientific simulations restrict us to showing the things that are absolutely essential to the engineer," explains Rosen Center for Advanced Computing director C. Hoffmann. "This gives us a simulation that doesn't deliver much visual information to a layperson. Our animation takes that scientific model and adds back the visual information required to make it a more effective

communication tool." The new animated visualization owes a lot to computer science professor V. Popescu, who devised a translator application that establishes a connection between computer simulations and computer visualization systems to automatically render simulation information as a three-dimensional animated scene. The animation clearly represents elements, such as fire and smoke, that were not included in the scientific simulation, imbuing the computer model with a previously absent level of realism, according to Popescu. The visualization shows that most of the damage to the towers was caused by the weight of the fuel carried by the aircraft that slammed into the buildings, and not the aircraft themselves. The National Science Foundation partially funded the Purdue research.

Hardware Designed to Protect Data From Theft By Hackers
Chicago Tribune (06/11/07), J. Van

In an effort to make computers more secure and reliable, University of Illinois at Urbana-Champaign researchers have been working for more than a year on the Trusted ILLIAC project, an effort to develop hardware that is capable of configuring itself to give each application a unique signature. The hardware cannot be reprogrammed by hackers and creates a barrier to protect sensitive data. "Hackers cannot reprogram it, and even insiders cannot access this data," says Ravi Iyer, chief scientist of the university's Information Trust Institute. "If they try to access it, they crash the application. They cannot corrupt it or even touch it." The National Science Foundation provided funding for the project, and university researchers also worked with researchers from Motorola, IBM, Hewlett-Packard, and Intel. Iyer says prototypes of the hardware could be made into cards that could be inserted into computers, but incorporating the hardware in processors is a more likely use of the technology.

Laws Threaten Security Researchers
Dark Reading (06/08/07)

The Computer Security Institute (CSI) recently formed a working group of Web researchers, computer crime law experts, and US Dept. of Justice agents to discuss the possible effects laws might have on Web 2.0 vulnerability research. The group's first report highlights the fact that some Web researchers said that if they accidentally find a bug on a site, they may not inform the Web site's owner for fear of prosecution. While security researchers are freely able to find bugs in operating systems, device drivers, and other applications on their own machines, Web researchers trying to find bugs on Web servers are dangerously close to violating laws designed to prevent hackers from tampering with Web servers' machines, and are afraid of the repercussions. The report analyses several methods of Web research, including off-site information gathering about a Web site, testing for cross-site scripting by sending HTML mail from the site to the researcher's Web-mail account, intentionally causing errors on the site, and conducting port scans and vulnerability scans. A Justice Department representative said that using only one of these methods might not provide enough evidence for a case against a hacker, and that it would require evidence of several of these techniques, along with evidence of attempts to hide such activity, to create a case. The CSI working group's next objective is to explore disclosure policy guidelines and mirrored-site guidelines for Web site owners. The group is also creating a list of research methods so lawmakers and law enforcement can have a better understanding of Web research methods.