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

Δελτίο 126
25 Αυγούστου 2008

Judge Refuses to Lift Gag Order on MIT Students in Boston Subway-Hack Case Computerworld (08/14/08), J. Vijayan

A trio of Massachusetts Institute of Technology (MIT) students discovered several security vulnerabilities in the electronic ticketing system used by Boston's mass transit authority, but they are not allowed to publicly discuss these vulnerabilities because of a temporary restraining order that US District Judge G. O'Toole refused to lift at the latest hearing on Aug. 14. The gag order will remain in effect until at least Aug. 19, when O'Toole is scheduled to hold another hearing on the case. The Electronic Frontier Foundation (EFF) says O'Toole asked the students to submit a copy of a class paper in which they detailed the vulnerabilities, along with copies of the programming code that they included in a planned presentation to demonstrate how the Massachusetts Bay Transportation Authority's (MBTA) e-ticketing system could be hacked. The gag order was granted when the MBTA filed suit to prevent the disclosure of the vulnerabilities, arguing that it was forced to seek court intercession because neither MIT nor the students had provided it with sufficient information to evaluate the vulnerabilities that were about to be publicly revealed at the Defcon hacker convention. The EFF filed a motion in court requesting that O'Toole lift the order, contending that it constitutes a violation of the students' First Amendment rights as well as a prior restraint on free speech. The decision to issue the restraining order was sharply criticized by Carnegie Mellon University professor D. Farber, who says he found the move especially deplorable in view of the fact that the students' paper was vetted by MIT professor R. Rivest.

Experts Accuse Bush Administration of Foot-Dragging on DNS Security Hole
Wired News (08/13/08), R. Singel

Security experts charge that bureaucratic lassitude at the US Department of Commerce's National Telecommunications and Information Administration (NTIA) is responsible for a major, lingering security hole in the Internet's domain name system (DNS). Experts and the NTIA concur that DNSSEC, a series of security extensions for name servers, is the only solution for a flaw that allows hackers to redirect Web traffic at will by feeding fake information into DNS listings. DNS servers function in a massive hierarchy, which means that the successful deployment of DNSSEC requires having a trustworthy party sign the root file with a public-private key. "The biggest difference is that once the root is signed and the public key is out, it will be put in every operating system and will be on all CDs from Apple, Microsoft, SUSE, Freebsd, etc," says Sparta's R. Mundy. NTIA's refusal to implement DNSSEC is a purely political move, as the technical difficulties of implementation have been addressed, says Packet Clearing House research director B. Woodcock. NTIA's B. Forbes says the administration has a responsibility to explore all possible solutions with all stakeholders before committing to DNSSEC, while even the most committed DNSSEC advocates acknowledge that Internet-wide installations of the extensions will consume a lot of time and money. The Internet Assigned Numbers Authority has spent the last year prototyping a system to sign the root-zone file, but it requires approval from the Commerce Department to do the same for the top Internet servers, at which point the issue becomes politically charged "because there

seems to be the perception that the introduction of a key guardian changes the current policies," says Dutch networking expert O. Kolkman.

Can Avatars Stop Identity Theft?
Salon.com (08/05/08), D. Caruso

Digital avatars like those that inhabit massively multiplayer online role-playing games such as Second Life may be crucial to restoring people's control over their digital identities. Businesses currently call the shots and basically force consumers to disclose whatever personal information they want so that they can purchase products and services, while a core element of such virtual worlds is the ability to conduct credible and anonymous transactions through avatars. Blogger D. Caruso says virtual worlds are an excellent testbed for the possibilities of user-centric identity systems. "Even at their relatively crude stage today, the technology on which they are based already allows them to interact and transact anonymously--with varying degrees of intimacy and in relative security--with millions of other avatars, including those who are hellbent on causing them some kind of digital harm," she notes. Identity Woman blog operator K. Hamlin predicted at the 2007 Digital ID World conference that avatars will eventually demand or be granted other digital rights, including the legal right to exist in the virtual rather than the physical domain. Identity professionals are investigating how to construct a less intrusive network that lets people drive their own identities around the Internet with a greater degree of safety. "Avatar technology has a long way to go before it can be truly useful as an identity system, but based on the trajectory of technology adoption--from enthusiast to professional to mass adoption--it is probably on the right course," Caruso concludes.

Patch for Web Security Hole Has Some Leaks of Its Own
New York Times (08/09/08) P. B1; J. Markoff

A Russian physicist has demonstrated that the emergency patch for the flaw found in the Domain Name System (DNS) is itself vulnerable. In a blog posting, physicist E. Polyakov wrote that he managed to get the patched DNS software to return an incorrect address in just 10 hours using two standard desktop computers and a high-speed network link. Internet experts who have reviewed Polyakov's work say the approach appears to be effective. The vulnerability of the DNS has been a hot topic since security researcher D. Kaminsky notified a number of Internet companies about the flaw earlier this year. Kaminsky recently said the DNS flaw also could affect other Web services, including email. Although the risk of such a flaw has been known for some time, last month security engineers repeatedly stated that it is only a matter of time before financial organizations and others are attacked through the flaw. Packet Clearing House research director B. Woodcock says there will almost certainly be an escalating number of attacks. "We have already been seeing attacks in the wild for the past two weeks," Woodcock says. Experts say the root of the problem is that modern networks are relying on an addressing system that was invented in 1983 and was not meant for services such as electronic banking that require strict identity verification. "They are relying on infrastructure that was not intended to do what people assume it does," says University of Southern California Center for Computer Systems Security director C. Neuman. "What makes this so frustrating is that no one has been listening to what we have been saying for the past 17 years."

Web Privacy on the Radar in Congress
New York Times (08/11/08) P. C1; S. Clifford

Questions surrounding online data collection and Internet user privacy are starting to attract the attention of Congress. Currently, there is no broad privacy legislation governing advertising on the Internet, and how companies use personal information collected from Internet users' Web habits is largely unknown. Even some in the government admit that they do not have a thorough understanding of what companies are able to do with the amount of data available to them. "That is why Congress, at this point, is wanting to gather a lot more information, because no one knows," says Vanderbilt University professor S. Hetcher. "That information is incredibly valuable; it's the new frontier of advertising." Many believe that companies should tell Internet users how their information is being tracked and used, but what area of the law covers this problem, and what regulation would look like, is still undecided. As advertisers become more sophisticated, and online privacy standards become increasingly varied, regulators and privacy advocates are becoming more concerned. Some companies have responded to concerns and criticisms, with Yahoo! and Google giving users the opportunity to opt out of targeted ads, but such a small change may not be enough. Rep. E. Markey (D-Mass.) says some type of omnibus electronic privacy legislation is needed, regardless of the technologies or companies involved. The Federal Trade Commission has proposed creating standards for behavioral-advertising practices in which companies would provide a clear notice to consumers that lets them choose not to be tracked, notify consumers if the company changes how it uses data, and requires companies to deploy reasonable security measures.

Ohio Official Sues E-Voting Vendor for Lost Votes
IDG News Service (08/08/08), G. Gross

Premier Election Solutions defended its electronic-voting machines after Ohio Secretary of State J. Brunner sued the vendor for dropping votes during the state's primary election in March. Although Premier did not respond directly to the lawsuit, a spokesman for the company formerly known as Diebold Election Systems said it offers high-quality voting systems that have had tremendous success in the state. The lawsuit is a counterclaim to a suit filed by Premier in May seeking a judgment that the company did not violate any contracts or warranties. After Butler County discovered that 150 votes were dropped, a statewide investigation found that hundreds of votes were dropped in 11 other counties. Brunner is suing Premier for failing to fulfill its contracts, and for breach of warranty and fraud. Her office issued a report in December that says the state should abandon touch-screen e-voting machines because of the "critical security failures" of the products of Premier and 2 other vendors. Premier blamed the problems on human error or conflicts with antivirus software in its own report in May.

Researchers Develop Next-Generation Antivirus System
University of Michigan News Service (08/05/08), N. C. Moore

CloudAV, a new cloud computing approach to malicious software detection developed at the University of Michigan (UM), could eliminate the need to install and update antivirus software on personal computers. CloudAV moves antivirus functionality into the network cloud and off of personal computers, and analyzes suspicious files using multiple antivirus and behavioral detection programs simultaneously. "CloudAV virtualizes and parallelizes detection functionality with multiple antivirus engines, significantly increasing overall protection," says UM professor F. Jahanian. To develop CloudAV, the researchers evaluated 12 traditional antivirus programs against 7,220 malware samples. Traditional antivirus software checks documents and programs as they are accessed, and because of performance constraints and program incompatibilities, typically only one antivirus program is used at a time. However, CloudAV can support a variety of malicious software detectors running in parallel to analyze

a single incoming file. Each detector acts as its own virtual machine, so technical incomepatibilities and security issues are not a problem. CloudAV is accessible to any computer or mobile device operating on the network that runs a simple software agent, and each time a computer or device receives a new document or program, the item is automatically detected and sent to the antivirus cloud for analysis.

Indiana University Department of Computer Science Study Shows Popular Web Sites at Risk for Phishers, Indiana University (07/30/08)

Indiana University School of Informatics researchers recently found that nearly 2.5 million Web pages on some of the Internet's most trusted and recognizable sites have 128,000 links that could be manipulated by phishers. Doctoral students C. Shue and A. Kalafut, along with their advisor, professor M. Gupta, developed a program that crawled tens of thousands of sites searching for and identifying open redirects, which are applications that take a parameter and redirect the user to the parameter value without any validation. These redirects serve a legitimate purpose, but they lack security controls and can be manipulated by phishers to send visitors to any site on the Internet. "We were surprised by the number of these open redirects on sites that people trust implicitly," Shue says. "When considering whether to click on links in email, users often look at whether the link goes to a trusted site. However, with redirects, phishers can manipulate the links to defraud these users." Shue presented the study's findings at the Usenix Workshop of Offensive technology.

Officials Say Flaws at Polls Will Remain in November
New York Times (08/16/08) P. A10; I. Urbina

The US Election Assistance Commission says that flaws in voting machines used by millions of people will not be fixed in time for the presidential election because of a government backlog in testing the machines' hardware and software. The flaws have created doubt over the ability of some machines to provide a consistent and reliable vote count, but commission officials say that they will not be able to certify that flawed machines are repaired by the November election, or provide software fixes or upgrades because of a backlog at the testing laboratories used by the commission. "We simply are not going to sacrifice the integrity of the certification process for expediency," says commission chairwoman R. Rodriguez. Consequently, machine manufacturers and state election officials say states and local jurisdictions are forgoing important software modifications meant to address security and performance concerns. In some cases, election officials in need of new equipment are being forced to buy machines that lack up-to-date upgrades. The federal government does not require that states use machines certified by the commission, but most states rely on the commission to approve new machines and software, and at least 10 states have rules or laws requiring federal certification. For example, Ohio requires federal certification, and although there is software available to correct the state's machines, the newer software cannot be used because it has not been certified. "We need the federal oversight to create consistent standards and to hold the manufacturers to a certain level of quality, but we also have to be able to get the equipment when we need it," says Ohio secretary of state J. Brunner. "Right now, that equipment is not coming, and we're left making contingency plans."

Some Russian PCs Used to Cyberattack Georgia
USA Today (08/18/08) P. 1B; B. Acohido

Thousands of Russian citizens have volunteered their PCs to be used in cyberattacks against Web sites supporting Georgia, say security experts. Several hours after skirmishes between Russia and Georgia started, a call for action was posted on the Web site stopgeorgia.ru, which listed Georgia government sites as potential targets. The site also posted a software tool that emits a stream of nuisance requests from the user's PC to target Web sites. Clicking on the tool allowed users to participate in a denial-of-service attack on Georgia's Web pages, says Damballa researcher A. Dinaburg. Thousands of pro-Russia users have been clicking on the tool and attacking a list of pro-Georgia Web sites. Russian cybercrime lords are also assisting Russia's assault by directing part of their large botnet networks to join the attack. Damballa recently identified a few hundred PCs in the United States that were also being used to attack pro-Georgia Web sites. A similar attack cut off most Internet services in Estonia for several weeks last year, and there have been at least a dozen smaller-scale attacks over political disputes between Russia and Baltic states with Western affiliations, says VeriSign's K. Zenz. "This type of attack will form at least a part of all geopolitical conflicts from now on," says Team Cymru's S. Santorelli.

Researchers Craft Multimedia Passwords
Techworld (08/14/08), J. Dunn

Canadian researchers have developed ObPwd, a new system that consumers can use to create secure passwords from images, MP3 files, or videos. With ObPwd (object-based password), consumers could use the picture of a cat to generate a sophisticated password that could not be cracked unless someone had access to the specific image or file used to generate the password. "Users keep a record [memorized or written] of a pointer to their content used in generating each password," writes Carleton University's M. and P. van Oorschot in a public paper on the approach. "Users can write down the password in a secure place, or re-create it from the content when needed." They would need to remember the file used to create the password, rather than a string of text. A software version has been released in beta form as an add-on tool for Mozilla, and as a standalone Windows XP utility. However, files that are too large could slow down the generation process, and creating passwords from public material such as pictures on a Facebook page or common image files is not recommended.

Before the Gunfire, Cyberattacks
New York Times (08/13/08) P. A1; J. Markoff

Weeks before any physical fighting occurred in the country of Georgia, a security researcher in Massachusetts observed a cyberattack against Georgia's Internet infrastructure. Arbor Networks' Jose Nazario noticed a stream of data directed at Georgia's government Web sites that contained the message "win+love+in+Russia." Other Internet experts say the cyberattacks against Georgia started as early as July 20, with distributed denial of service (DDOS) attacks overloading and effectively shutting down servers in Georgia. Researchers at Shadowserver, a volunteer group that monitors malicious network activity, reported that Georgia President M. Saakashvili's Web site was rendered inoperable for 24 hours due to multiple DDOS attacks, and that the control server that directed the attack was based in the United States and had come online only a few weeks before the attack started. It now appears that the July attack may have simply been a test run for a larger cyberwar between Georgia and Russia. In addition to DDOS attacks, researchers say there is also evidence that Internet traffic was redirected through Russian telecommunications firms. Experts say this is the first time a cyberattack has coincided with a physical attack. However, it is unlikely to be the last, says Packet Clearing House research director B. Woodcock, who notes that cyberattacks are inexpensive,

easy to execute, and leave so few fingerprints that they will almost certainly be a fixture in modern warfare. "It costs about 4 cents per machine," Woodcock says. "You could fund an entire cyberwarfare campaign for the cost of replacing a tank tread, so you would be foolish not to." Georgia experienced few adverse effects from the attack, other than a lack of access to government Web sites.

Web-Security Inventor Charts a Squigglier Course
Wall Street Journal (08/13/08) P. B5; E. Smith

Carnegie Mellon University professor L. von Ahn, the primary inventor of the Captcha online security test, has updated the system to make the test more secure. The new ReCaptcha system would also have users assist in the digitalization of old books and newspapers. The new system presents users with two words containing distorted characters. Both words are taken from an old book or newspaper article that has been scanned into an online library. One of the words was recognized by the scanning software, while the other was unrecognizable to the computer, possibly because of a smudge or some other imperfection on the original document. The user tries to decipher the distorted characters of both words, and if the user matches the first word correctly, which the computer already knows, then the user's reading of the unknown word is recorded. Multiple Web users will be shown the same unknown word as part of different tests, and when three people have submitted the same answer for the unknown word, it is considered solved and added to the library database to be inserted into the digital version of the document. Deciphering these unknown words is one of the greatest challenges for the Internet Archive library digitalization effort, since scanning software generally has an accuracy rating of only about 80% for books published before 1900. About 40,000 Web sites now use the free ReCaptcha system, and when fully operational, von Ahn expects it to process about 160 books a day for the Internet Archive. "It's a really mind-blowing application," says Internet Archive founder B. Kahle.

US at Risk of Cyberattacks, Experts Say
CNN (08/18/08), B. Griggs

The next large-scale military or terrorist attack against the United States may be launched by hackers half a world away through cyberspace, which Internet security experts say could be just as devastating to the US economy and infrastructure as a physical attack. Experts say the recent attacks on Georgia heralds a new kind of cyberwar, for which the United States is not fully prepared. Tulip Systems CEO T. Burling says that no one has developed a way to prevent such attacks from happening. "The US is probably more Internet-dependent than any place in the world," Burling says. "So to that extent, we're more vulnerable than any place in the world to this kind of attack." United States Cyber Consequences Unit director S. Borg says Internet security is a critical issue, and in the United States, at every level, security is dependent on computers. "It's a whole new era. Political and military conflicts now will almost always have a cyber component," Borg says. "The chief targets will be critical infrastructure, and the attacks will emerge from within our own computer systems." A major challenge is that such attacks can be launched anonymously, and relatively cheaply, from anywhere in the world. The US Dept. of Homeland Security created the National Cybersecurity Center this year to coordinate federal cyberdefense efforts and improve responsiveness, but a recent Homeland Security Department intelligence report concluded that there are currently no effective means to prevent a coordinated attack on US Web sites.