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

Δελτίο 115
5 Μάη 2008

FBI's Net Surveillance Proposal Raises Privacy, Legal Concerns
CNet (04/25/08), D. McCullagh

During a recent House Judiciary Committee hearing, the FBI's R. Mueller and Rep. D. Issa (R-Calif.) discussed a two-step approach for enabling warrantless surveillance of the Internet. The first step would involve asking Internet service providers to open their networks to the FBI voluntarily. The second step would involve creating a federal law that would require ISPs to do so. As part of the first step, Issa suggested that ISPs could get consent from all of their subscribers to allow federal police to monitor network traffic for attempts to steal personal information and national secrets. Mueller said legislation is needed for "some omnibus search capability utilizing filters that would identify the illegal activity as it comes through" and allow the government to preempt any illegal activity. The Center for Democracy and Technology's G. Nojeim says the effort is very troubling, and it could, through unknowing consent, cause Internet users to give permission to monitor communications in ways that would otherwise be illegal. The Electronic Communications Privacy Act says that providers may share the contents of customers' communications but only with the "lawful consent" of the user, but what constitutes lawful consent is still under debate. Even if ISPs agree to allow federal authorities to monitor their traffic, many states have far more stringent regulations that would make such activities illegal. How such laws would intersect with International users is also problematic. The problems created by wide-scale Internet surveillance under existing state laws may make creating a federal law a necessity, which would include re-writing US surveillance law.

Few States Take Email Votes From Troops
Associated Press (04/27/08), L/ Baldor

Troops in Afghanistan and Iraq have few options for casting their ballots in the upcoming presidential election. Communities in 13 states will send overseas troops presidential election ballots by email, and districts in at least seven states will allow troops to return the ballots over the Internet, according to the Associated Press and the Overseas Vote Foundation. However, tens of thousands of service members in foreign military bases still have no choice but to rely on regular mail to receive and cast ballots, which is often done at the last minute because of delays in ballot preparations in some states. Making the process more electronic would solve some of these problems, but doing so would also raise security and privacy concerns. Pentagon officials have encouraged more states to switch to electronic voting before November, which could help reverse recent trends in which thousands of military members have asked for ballots but either did not vote or had their ballots rejected because of flaws. "The personnel that fight our wars, the people who are most affected by the decisions on the use of the military, are being systematically denied the right to vote," says the Overseas Vote Foundation's B. Carey. Carey says that ballots are often not prepared and ready to be mailed until 30-45 days before an election, and it can sometimes take more than two weeks for troops to receive mail, meaning the ballots will arrive too late for their votes to count. Although the use of email voting is a controversial matter among the National Association of

Secretaries of State, Indiana Secretary of State T. Rokita says Indiana has had no problems using email to deliver and receive ballots from overseas voters.

Florida Alters Its Voting Laws, But New Disputes May Emerge
New York Times (04/28/08) P. A1; D. Cave

Florida state lawmakers have passed several laws since the 2000 presidential recount in an effort to bring order to their election system, but many believe the laws may only create more chaos. Three laws in particular are at the center of a heated debate. The first law is a "no match, no vote" provision that rejects potential voters if their Social Security number or driver's license number does not match the number in the state database. By 2006, at least 11 states had created "no match, no vote" provisions, but a judge in Washington state struck down a "no match, no vote" law in 2006, and at least six other states have abandoned similar provisions. The second law creates deadlines and fines of up to $1,000 for third-party groups that lose voter registration forms or turn them in late. The law has forced many organizations to stop voter registration efforts to protect themselves from liability. The third law prohibits voters from correcting mistakes or omissions on voter registration forms in the final month before an election, even if those mistakes or omissions might bar them from having their vote count. Such oversights can be as simple as missing a check box. Voters are now allowed to amend registration forms after the deadline in 33 states. Many believe the Florida laws are biased against poor, black, and Hispanic voters, and attempt to block new voters. "It's really about politicians trying to game the system," says Project Vote deputy director M. Slater. "They have done that by adding all these bureaucratic obstacles to voting, and then when people cannot jump over them, they blame the voter."

Patches Pose Significant Risk, Researchers Say
SecurityFocus (04/23/08), R. Lemos

A team of computer scientists has developed a technique that exploits patches and updates by automatically comparing the vulnerable and repaired versions of a program and creating attack code. The technique, which the researchers call automatic patch-based exploit generation (APEG), can generate attack code for most major vulnerabilities in minutes by automatically analyzing a patch design to fix a flaw. If Microsoft does not change how it distributes patches to customers, attackers could create a system that attacks the flaws in unpatched systems minutes after an update is sent out, says Carnegie Mellon computer science PhD candidate D. Brumley. The technique is built on methods used by many security researchers, who reverse engineer patches to find vulnerabilities fixed by the update. Normally the process can take a few days, or even hours, but Brumley and his colleagues were able to use APEG to create exploits in five recent Microsoft patches in under six seconds each time. The system does not create fully weaponized exploits and may not work on all types of vulnerabilities, but it shows that developing exploits from patches can be done in minutes. The researchers suggest that Microsoft could increase the likelihood that customers receive patches before attackers can reverse engineer them by obfuscating the code, encrypting the patches and waiting to distribute the key simultaneously, and using peer-to-peer networks to increase the distribution of patches.

Shibboleth Authentication Tool Upgraded
Government Computer News (04/22/08), W. Jackson

Internet2 has released an upgraded version of Shibboleth, an open source identity management tool that is widely used in the academic research community to provide users with a secure, single-sign-on mechanism for accessing protected online resources from their campuses and external service provider partners. Among the additions Internet2 made to Shibboleth is an implementation of the OASIS Security Assertion Markup Language (SAML) 2.0 standard, which includes security features such as encryption technology. Also included in SAML 2.0 is a better method for usage logging at the home institution. This will allow for better tracking of abuse or inappropriate use of the system. The new version of Shibboleth also includes improved anonymous identifiers, which were used in the previous version of the software to protect user privacy. With the new version of Shibboleth, identity providers can assign a persistent unique identifier to a specific user, which in turn will allow service providers to better meet the needs of that user without knowing his specific identity. Students researching articles in an online medical journal, for example, will be able to use the anonymous identifier to save their searches and add to their research over time.

One Breach Is One Too Many in Cyber Warfare
Monterey County Herald (CA) (04/29/08), K. Howe

Students from the Naval Postgraduate School's computer science department, along with students from the Army, Navy, Air Force, Coast Guard, Merchant Marine service academies, and the Air Force Institute of Technology recently tested their cyberspace defensive abilities against a team of computer hackers from the National Security Agency. In its eighth year, the annual cyberwar exercise is intended to give students a chance to "get their hands dirty" while learning about vulnerabilities in computer systems, says Naval Postgraduate School senior lecturer Scott Cote. The students were given computers that had compromised programs that needed to be found before they were exploited by the NSA hackers. The students were limited to defensive strategies only, and were given a limited budget for hardware and firewall software to add to the realism of the exercise. Only one cyber attack from NSA got through the NPS firewall during the four-day exercise, but Cote says it only takes one mistake for hackers to wreck an entire system. The Air Force Institute of Technology was the top scorer, Cote says, and the undergraduate teams did not do as well, but that is because they do not have as much experience. However, he says students come away with an understanding of how systems can be attacked, the amount of damage that can be done, and how to prevent attacks.

Information Security Set for Explosive Growth
Campus Technology (04/24/08), D. Nagel

Compliance and public confidence issues will cause information security to dramatically expand over the next few years, predicts a Frost & Sullivan and $(ISC)^2$ report. Worldwide, the number of information security professionals is expected to increase from 1.66 million in 2007 to about 2.7 million by 2012. The report says that, as a percentage, most of the growth will occur in Europe, the Middle East, and Africa, though the Americas will dominate in raw numbers, expanding from 685,700 professionals in 2007 to more than 1.1 million in 2012. The 2008 $(ISC)^2$ Information Security Workforce Study polled 7,548 respondents from the public and private sectors in the fall of 2007. The report says that forces driving the expansion of information security include regulatory compliance initiatives that make executives responsible, organizations' needs to prevent damage to their reputation and to maintain public confidence, and possible financial losses for failing to meet regulatory requirements. Frost & Sullivan estimates that the potential cost of a data breach varies between $50-$200/sec record

lost, not including intangible losses that result from damage to the organization's reputation. The top security concerns include intrusion prevention, risk management solutions, vulnerability assessment and penetration testing, and incident management. To support these technology and security goals, 40% of respondents said that they will personally acquire additional certifications within the next 12 months.

Critical Infrastructure Central to Cyber Threat
Federal Computer Week (04/24/08), B. Bain

Cybersecurity specialists at the GovSec, US Law and Ready Conference and Exposition in Washington, warned that the nation is increasingly prone to cyberattacks that could have a disastrous effect on vital physical infrastructure. Among those in attendance at the event was US-CCU director S. Borg, who said that scalable cyberattacks could destroy a large number of electricity generators that would take years to replace. Such an event would likely result in deaths as well as an economic calamity. "We are talking about things much bigger than the Great Depression," Borg says. "We are talking about consequences that are only exceeded by use of nuclear weapons." Borg also voiced concern about the federal government's efforts to consolidate access points to its systems - efforts he said could make those systems more vulnerable to damage from attacks. He added that cybersecurity and military efforts should begin to focus on resiliency, creating robust systems, and protecting critical infrastructure instead of focusing solely on perimeter defenses.

Experts Struggle With Cybersecurity Agenda
Government Computer News (04/28/08), W. Jackson

The Commission on Cyber Security for the 44th Presidency, established in November by the Center for Strategic and International Studies (CSIS), recently held the second of five scheduled public meetings to field recommendations on issues surrounding information security, identity theft, and government leadership. CSIS established the commission to create recommendations for a comprehensive strategy to improve federal systems and critical infrastructure cybersecurity. The objective is to have a set of recommendations ready for the next president by November. Panelists at the meeting said leadership is needed from the government and industry to create a public/private partnership to create adequate security. Although they were not in complete agreement on cybersecurity priorities, they did agree that a single national data breach notification law is needed to replace the patchwork of more than 40 state laws. Other topics included creating a zero-tolerance policy for identity theft and requiring verification for online transactions with consumers, requiring the Social Security Administration to create a database linking Social Security numbers with dates of birth to prevent the misuse of Social Security numbers, and establishing an International Data Classification Standard to help identify and assess value and risk to data.

Digital Deception
Washington Post (05/01/08) P. D1; P. Whoriskey

Human-mimicking computers are becoming increasingly successful at solving CAPTCHA online tests intended to separate humans from computers. In April, Hotmail CAPTCHAs were broken by a computer. The computer then created numerous free Hotmail email accounts and sent out waves of spam, Websense says. Similar attacks occurred this year at Microsoft's Live Mail and Google's Gmail and Blogger. "What we're noticing over the last year is that these tests meant to tell the difference between a human and a computer are being targeted by

more and more malicious groups," says Websense's S. Chenette. "And they are getting better at it." Solving CAPTCHAs with computers allows spammers to quickly create new email accounts to send spam, which Ferris Research estimates could cost the US economy $42 billion annually. In addition to computers breaking CAPTCHAs, low-wage workers overseas are being paid to solve them. In fact, Google says it believes humans were involved in solving its CAPTCHAs. Microsoft and other Web companies say they are interested in developing human verification tests that are more difficult for computers to crack, but making the tests harder for a computer could make them harder for humans as well.

Malicious Hardware May Be Next Hacker Tool
New Scientist (05/01/08), M. Inman

Hackers could soon start using a new tactic in which they gain control of a computer by adding malicious circuits to its processor, say University of Illinois at Urbana-Champaign researchers. The malicious circuits would be able to avoid detection because they could manipulate computers at a deeper level than a virus. A University of Illinois at Urbana-Champaign research team led by professor S. King used a field programmable gate array (FPGA) to create a replica of an existing open source processor with about 1.7 million circuits. The team added about 1,000 malicious circuits not present in the processor. The malicious circuits allowed the team to bypass security controls on the processor similar to how a virus gives control to a hacker, but without requiring a software flaw. Attaching the FPGA to another computer allowed them to steal passwords stored in its memory and install malicious software that would give them remote control of the computer's operating system. Putting malicious hardware on a chip is not as easy as installing a virus, as the hacker must have either access to a chip during its design or manufacturing, be able to build and sell those chips to a computer manufacturer, or sneak their chips into computers during assembly. However, as chips and their design processes become more complex, it becomes easier for a hacker to infiltrate.

Beating the Codebreakers With Quantum Cryptography
ICT Results (04/28/08)

Cryptography has been an arms race, with codemakers and hackers constantly updating their arsenals, but quantum cryptography could theoretically give codemakers the upper hand. Even the absolute best in classical encryption, the 128-bit RSA, can be cracked using brute force computing power. However, quantum cryptography could make possible uncrackable code using quantum key distribution (QKD). Modern cryptography relies on the use of digital keys to encrypt data before sending it over a network so it can be decrypted by the recipient. QKD promises a theoretically uncrackable code, one that can be easily distributed and still be transparent. Additionally, the nature of quantum mechanics makes it so that if an eavesdropper tries to intercept or spy on the transmission, both the sender and the receiver will know. Any attempt to read the transmission will alert the sender and the receiver, allowing them to generate a new key to send securely. QKD had its first real-world application in Geneva, where quantum cryptography was used in the electronic voting system. Not only did QKD guarantee that the poll was secure, but it also ensured that no votes were lost in transmission, because the uncertainty principle established that there were no changes in the transmitted data. The SECOQC project, which did the work for the voting system, says the goal is to establish network-wide quantum encryption that can work over longer distances between multiple parties.

Phantom Obama Vote Appears on NJ Voting Machine
Wired News (04/30/08), K. Zetter

Officials from New Jersey's Pennsauken District 6 report that 279 votes were cast during the Feb. 5, 2008, Democratic primary, but Princeton University computer scientist E. Felten has learned that a phantom vote was cast for Barack Obama. The county clerk's report is based on information taken digitally from the memory cards inside three Sequoia voting machines. However, Felten says the summary tapes printed from the machines show that there were 280 votes, and Obama received 95 rather than 94 votes. Felten has a better chance of solving the mystery surrounding the Sequoia voting machines after a judge ruled last week that independent experts could gain access to voting machines in order to test their software and firmware. The ruling stems from a lawsuit filed in 2004 over the legality of using touch-screen voting machines in the state. Sequoia had threatened to sue the state if it allowed researchers such as Felten to review its machines.

Social Networking Applications Can Pose Security Risks
Associated Press (04/28/08), M. Irvine

The thousands of mini-programs designed by third-party developers for use on social networking sites such as Facebook and MySpace could pose a security risk for users. Such programs are risky for users in part because they can be created by anyone with a little technical know-how to gather information about the users who download them. Among those who have created a social networking application is A. Felt, a Facebook user and a computer science student at the University of Virginia who wanted to research how such applications work. As part of her research, Felt polled developers of the application and found that they did not use or need the information they gleaned from users who downloaded their applications, includeing demographic information such as gender and age. Developers that did use the information said they only used it to display targeted ads to the person when they used the application. However, Felt found that there was nothing stopping developers from matching the information they gathered with public records. But even more worrisome for social networking users is the prospect that the information gathered by developers could be sold or stolen, which could in turn lead to identity theft. Applications are not the only threat to social networking users. Last year, researchers from Indiana University found that they were able to "scrape" information from students' social networking sites. Given these threats, social networking users should limit the information they post on their pages, said T. Jagatic, one of the researchers involved in the Indiana University study.