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

Δελτίο 21
20 Απρίλη 2006

Report Details DMCA Misuses
InternetNews.com (04/14/06), D. Miller

The Electronic Frontier Foundation (EFF) has issued a report criticizing many of the misuses of the Digital Millennium Copyright Act, the 1998 law enacted to safeguard intellectual property in the digital era. Among the stories included in "Unintended Consequences: Seven Years Under the DMCA" is graduate student J. Halderman's account of how he waited several weeks before going public with his discovery of the Sony rootkit vulnerability so that he could consult with his attorneys. SunComm executives had threatened Halderman with a DMCA suit in 2003 after he discovered a vulnerability in that company's copy-protection technology. "Rather than being used to stop piracy, the DMCA has predominantly been used to threaten and sue legitimate consumers, scientists, publishers, and competitors," said the EFF's Fred Von Lohmann. The report takes particular issue with Section 1201 of the DMCA, which bars the circumvention of DRM technologies, even in cases when circumvention would be logical and legitimate, such as security research. Violators of the DMCA can face severe civil and even criminal penalties. The EFF report calls for support for the Digital Media Consumers' Right Act, introduced by Rep. R. Boucher (D-Va.) in March 2005, requiring that a CD must plainly state on its label if its content has been copyright-protected, as well as the return policy for the CD in the event that it does not play properly because of the copyright-protection technology. The Consumer Electronics Association also supports Boucher's bill. "We believe that the DMCA is overly broad," said the association's M. Petricone. "It's a major burden on legitimate innovation and research that chills normal and customary consumer conduct." Others argue that while the DMCA is imperfect, the stories of abuse are vastly outnumbered by the millions of legal downloads that the DMCA has helped protect against illegal copying.

Does Every Vote Count?
San Antonio Express-News (TX) (04/09/06), R. Chapa

In the wake of recent contentious elections that ended up in a recount of paper ballots, computer experts have been calling for a nationwide mandate that would require all e-voting machines to produce a paper trail. "You can't trust an election that's run with paperless machines," said Avi Rubin, computer science professor at Johns Hopkins University. "There isn't any way to recover the results." Currently, 25 states require their voting machines to contain a voter-verified paper trail, though more are having to wrestle with the issue as they race to purchase new equipment under the 2002 Help America Vote Act. Rep. R. Holt (D-NJ) has introduced legislation that would require every precinct to use machines that produce a paper trail and each state to conduct unannounced audits of 2% of its jurisdictions. The US General Accounting Office released a report in September touting the potential of e-voting machines to improve the election process, though it mentioned the numerous warnings that have raised "concerns about their security and reliability." If election results are contested, Rubin and Stanford computer scientists D. Dill argue that without a voter-verified paper trail, auditors will only be able to reprint the ballots, which would simply reproduce the same errors that the machines made on election day. Nevada has implemented machines with voter-verifiable paper trails in each of its 17 counties, and has met with positive feedback from voters. In Leon County, Fla., elections administrator I. Sancho sparked controversy last year when he invited security researchers to attempt to hack into the county's Diebold machines. While the security experts succeeded in penetrating the system, Diebold lashed out at Sancho, calling his tests "foolish and irresponsible." With counties throughout the country scrambling to implement new systems, vendors are also having difficulty keeping up with demand.

Big Brother Is Listening
Atlantic Monthly (04/06) Vol. 297, No. 3, P. 65; J. Bamford

Technological advancements have widened the scope of National Security Agency (NSA) surveillance, while the legal barriers to such eavesdropping have been lowered with a White House mandate that permits the NSA to place Americans on watch lists and monitor their communications without first obtaining permission from the Foreign Intelligence Surveillance (FISA) court. Previously a court order was required, and could only be secured if the NSA showed that it had probable cause to eavesdrop on people suspected of involvement with terrorist organizations. Now people can be placed on watch lists by NSA shift supervisors who have a "reasonable belief" of involvement, and the number of Americans targeted by the NSA has consequently ballooned from perhaps 12 annually to 5,000 over the last 4 years, according to sources. If innocent people are marked because they fulfill these highly subjective criteria, they may be denied visas, federal jobs, or other services and privileges without ever knowing why. The NSA's surveillance methodology is signal intelligence, in which electronic communications containing vast quantities of emails and phone calls are intercepted and run through computers that flag specific words, phrases, names, phone numbers, and Internet addresses, and forward these communications to analysts. Also clearing the way for greater NSA surveillance is the FCC's extension of the 1994 Communications Assistance for Law Enforcement Act (CALEA) to cover "any type of broadband Internet access service" and new Internet phone services, while the two congressional intelligence committees tasked with protecting the public from privacy abuses have abnegated their responsibilities. The NSA likes to hire people away from providers of critical telecommunications system components, offering them the opportunity to work with state-of-the-art equipment and contribute to national security. Furthermore, a great deal of the telecommunications industry secretly cooperates with the NSA in its eavesdropping efforts.

New RFID Travel Cards Could Pose Privacy Threat
CNet (04/18/06), D. McCullagh

The embedded computer chips that might be used in government-issued travel cards can be read at a distance up to 30 feet, according to J. Williams, director of the Department of Homeland Security's US-VISIT program, posing a potential threat to privacy. The chips, which use RFID technology, could appear in cards used by Americans to enter Canada and Mexico as early as 2008. Privacy advocates have already voiced concerns about RFID technology, and a California politician has introduced legislation restricting its use. The concerns diminish with chips that can only be read from a few inches, though at a distance of 30 feet, sensors hidden along a road could theoretically read them, as could a stranger passing on a street. The disputed cards are known as "PASS" (People Access Security Service), and are being issued as part of a government initiative requiring anyone traveling over the Canadian or Mexican border to carry alternative travel documentation. A government procurement notice issued by the Department of Homeland Security stipulated that the devices be readable from a distance of at least 25 feet, and that the "IDs be read under circumstances that include the device being carried in a pocket, purse, wallet, in traveler's clothes, or elsewhere on the person of the traveler." The State Department appears to prefer a proximity-based card, rather than a remotely readable RFID-enabled device. RFID chips will already begin appearing in US passports in October, and proposals to implant them in driver's licenses have met with staunch opposition from privacy advocates. Despite similar criticism of the e-passport initiative, the State Department's F. Moss says the chips used will only be readable from 10cm, and will contain a sophisticated cryptographic technique known as basic access control.

Code for 'Unbreakable' Quantum Encryption Generated at Record Speed Over Fiber
NIST News (04/18/06)

Researchers at the National Institute of Standards and Technology (NIST) have generated raw code for quantum encryption at a record speed of more than 4 Mbps over 1km of optical fiber, doubling NIST's previous record. Using individual photons of different orientations to create a steady binary code, or encryption key, the NIST quantum key distribution (QKD) method could lead to ultra-secure transmissions of video and other data over conventional high-speed networks. The researchers attained the record with only a 3.6% error rate, and look toward the next step of processing the raw key to produce a secret key at roughly 2 Mbps. "This is all part of our effort to build a prototype high-speed quantum network in our lab," said NIST physicist Xiao Tang. "When it is completed, we will be able to view QKD-secured video signals sent by two cameras at different locations. Such a system becomes a QKD-secured surveillance network." Though tested over a shorter distance, the NIST system operates faster than previously reported systems developed by other groups. Through two channels linking two PCs in a lab over optical fiber, the system transmits photons in their quantum states representing ones and zeros, adjusting for changes in environmental conditions such as temperature and vibration. Once the system creates and processes the raw key, it uses the secret key to encrypt and decrypt video signals. Lasers produce a series of single photons in the NIST system, which carry the raw material for the quantum key over the fiber via a one-way channel. The researchers had to develop a workaround to correct the distortion of the sending computer's photons that occurred when they passed over curved fiber. Once corrected, the key is hashed in a privacy amplification technique that ensures only the sender and intended recipient will see the key in its entirety.

Bringing Free Software to the Masses
ZDNet UK (04/13/06), I. Marson

In a recent interview, P. Brown, the executive director of the Free Software Foundation (FSF), discussed his thoughts on the forthcoming draft of the GPL and the foundation's campaign to end digital rights management (DRM). Brown claims not to have written a program since he was 14, instead bringing a background in management and finance to the FSF when he took a part-time job there in 2001 doing mostly administrative work. Brown eventually took on more responsibility, managing the GPL compliance lab before being elevated to executive director of the foundation in February. One of Brown's main challenges is promoting the foundation's mission in the mainstream press, so that the message of free and open computing stretches beyond the strictly technical community. With the second draft of GPLv3 forthcoming in June, Brown says that will be "the first stake in the ground against DRM," noting that the campaign against digital restrictions is all the more timely with the upcoming Windows Vista and the recent revelations that certain CDs will not play on certain players because of DRM. Though the campaign will not be overtly political, Brown notes that there is some poor legislation that should be changed, but that the FSF, with the help of a professional campaigner, will focus more on mobilizing people at a grass-roots level to boycott products or picket certain organizations. Brown also noted that, unlike other free or open-source projects, the FSF is highly legalistic, and believes that securing its assets through copyright agreements with developers is crucial to protecting computing freedom. The FSF generates revenue through membership, donations, and selling merchandise such as t-shirts and books, and its founder and director, R. Stallman, refusing to take a salary, lives off speakers' fees and award money.

DHS Still Gearing Up Response to Cyberthreats
Government Computer News (04/17/06), W. Jackson

US Homeland Security Department (DHS) acting director of National Cybersecurity A. Purdy says the United States faces serious vulnerabilities to cyber-attack and the department still has a long way to go in addressing this problem. Purdy, speaking at the 2006 International Conference on Network Security, says the department wants to create a plan for how to organize a quick response to a significant cyber-attack. Its second priority is to develop a way to disseminate cybersecurity and attack-related information among government agencies and companies. DHS has been working with the IT industry to forge a comprehensive protection plan for critical national IT infrastructure, but it has yet to get far. Purdy says such efforts are hindered by a lack of organization. He says, "There are so many players, so many different people doing different things." DHS also recently created a cybersecurity position at the level of DHS assistant secretary, and Purdy says the department is working with the White House to fill it now.

Does Open Source Encourage Rootkits?
Network World (04/17/06) Vol. 23, No. 15, P. 1; E. Messmer

In its recently published report, "Rootkits," McAfee identifies a ninefold increase in the number of rootkits collected as samples of malware this quarter compared with the same time last year, attributing the spike to the activities of the open-source community. Nearly all the rootkits McAfee identified are designed to conceal code, such as spyware or bots, or to mask applications operating in Windows systems. "The predominant reason for the growth in use of stealthy code is because of sites like Rootkit.com," said McAfee's Stuart McClure. Rootkit.com has 41,533 members who anonymously post rootkit source code, though site operator G. Hoglund claims the site exists as a resource for anti-virus firms and others who want to learn about rootkits, but that anyone with strictly malicious motives would be foolish to post on the site, because the rootkit would be held up to public scrutiny and detection. Hoglund admits, though, that with tens of thousands of users, there are likely to be some people who are more interested in exploiting vulnerabilities than using the site for educational purposes. Because it draws on a massive brain trust, the open-source community is critical to exposing new vulnerabilities and developing better code, says TrendMicro's D. Perry, who nevertheless allows that Rootkit.com attracts a lot of would-be hackers who use it to shop for tools. Hoglund says there are probably only 20-30 main types of rootkits, though there are numerous variants. Rootkit detection and eradication have become frontiers in software research, and while some rootkits are nearly impossible to eradicate, Rootkit.com has made it easier for people to use the software designed to find and eliminate them, said Komoku CTO J. Butler. A major fear in the security industry is that a hacker will soon be able to scan networks with a worm and deliver a piece of malware that could wipe out files or alter data while remaining hidden by a rootkit.