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

Δελτίο 26
26 Μάη 2006

Congress May Make ISPs Snoop on You
CNet (05/16/06), D. McCullagh

House Judiciary Committee Chairman Rep. F. Sensenbrenner (R-Wis.) is set to introduce legislation as early as this week that would require ISPs to record information about US Internet users' online activities so that police can more easily "conduct criminal investigations." The legislation--called the Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act--is likely to be controversial because it would significantly change US laws regarding the protection of Americans' Web surfing habits. ISPs currently discard any log file that is no longer required for business reasons such as network monitoring, fraud prevention, or billing disputes, although they do make exceptions when contacted by police conducting an investigation. Critics such as Electronic Privacy Information Center executive director M. Rotenberg says Sensenbrenner's legislation is too vague. Instead of specifically describing exactly what information ISPs would be required to keep about their users, the legislation gives the attorney general broad discretion in drafting regulations. At minimum, the proposal says, user names, physical addresses, IP addresses, and subscribers' phone numbers must be retained. That generous wording could allow the attorney general to order ISPs to keep records of email correspondents, Web pages visited, and even the contents of communications. Despite the controversy, the legislation has garnered the support of state law enforcement agencies, which say strict data retention laws will help them investigate crimes that have taken place awhile ago.

More E-Voting Concerns Surface With State Primaries Underway
The NewStandard (05/17/06), C. Komp

State and local officials are increasingly joining voting-rights groups in questioning the security of e-voting systems, particularly since the recent discovery of a serious flaw in one of Diebold's touch-screen machines. The vulnerability comes from a feature that Diebold included to enable the machines to install software updates with ease, though security experts warn that the same feature could be exploited by anyone with a basic knowledge of the system who wanted to install software that could manipulate votes. Election officials have turned to the security community for independent analysis when Diebold's responses to their concerns have been unsatisfactory. "They just don't get it," said M. Shamos, professor of computer science at Carnegie Mellon University. "We've had many, many discussions. In fact, if you look at their public statements they've made in light of this revelation, it shows that they still don't get it." Diebold argues that tampering with the machines would require the involvement of a malicious election official, a possibility which the company discounts. Only California, Iowa, and Pennsylvania have addressed the Diebold problem so far, though many state use the systems. In Iowa, Deputy Secretary of State J. Hedgecoth ordered election officials to run a final software upgrade and seal the machine with a memory card inside immediately prior to the upcoming election. "So we are controlling both the software in the field with a final version that is decided upon by our elections division, and then we're securing the memory card against tampering on Election Day," Hedgecoth said. As concerns about e-voting systems in general have reached a fever pitch, voters in Arizona have filed a lawsuit to block

the state from purchasing systems that "are not trustworthy or transparent," following similar suits filed in California, New York, and New Mexico.

Nominee Says N.S.A. Stayed Within Law on Wiretaps
New York Times (05/19/06) P. A20; E. Lichtblau

Gen. M. Hayden, President Bush's nominee for CIA director, told a panel of senators at his Senate confirmation hearing on Thursday that the National Security Agency (NSA) did not exceed the bounds of the law in carrying out secret wiretaps on international phone calls and email of Americans without warrants, as authorized by the president shortly after 9/11. Democratic senators bluntly questioned Hayden about the surveillance's legality and whether he had deceived Congress and the public about the program. Hayden referred to the program's legal and constitutional authority, and the need to keep its operations clandestine as being paramount to its effectiveness. He also mentioned his discussions with NSA lawyers about the program's legal viability under the president's authority as commander in chief under Article II of the US Constitution. According to Hayden, the lawyers "were very comfortable with the Article II arguments and the president's inherent authorities." However, he confessed his ignorance of the Justice Department's official opinion establishing the legal motivation for the program, and admitted his inability to recount any significant discussion about the congressional authorization in 2001 to apply all necessary force against Al Qaeda, which the White House now claims helped legally empower it to authorize the surveillance program. Hayden acknowledged that there was substantive talk within the Bush administration, and between the NSA and the White House, about carrying out the operation.

Academia Welcomes New Thinking on Foreign Researchers and National Security ResearchResearch (05/17/06)

The academic research community is happy that the Department of Commerce intends to delay proposed alterations to alleged "deemed export" rules, regulations that oversee and limit foreign researchers who work with sensitive items. The department will instead announce in the near future the establishment of an advisory panel to recommend ways of balancing national security with research and higher education interests. Association of American Universities Interim President J. Vaughn said that the initial IG suggestions would have delayed research and would have sent the message that leading global talent was not welcome. Vaughn stressed his association's stance that exemption from deemed export regulations for basic research should stay intact and that the exemption must also apply to the tools and technologies vital to the conduct of the research. Meanwhile, Carnegie Mellon University President J. Cohon said that it is crucial that any limits on fundamental research done in America's universities by foreign national be carefully reviewed as their contributions keep promoting the nation's economic well-being. In addition, the Computer Research Association stated in its blog that the department's decision is "a nice win for the science community."

Cyber Threats to U.S. Business Grow More Dangerous
Reuters (05/14/06), J. Rothstein

S. Borg, director of the Cyber Consequences Unit (CCU), says attacks on US computer networks are becoming more dangerous and could lead to the destruction of companies or even death. The CCU, which is funded by the Homeland Security Department, is trying to figure out how to prevent attacks in regards to plans to cause power blackouts, plots to tamper with pharmaceutical products, or schemes to reprogram machinery to build dangerously defective

products. "Up to now, executives and network professionals have been worrying about what adolescents and petty criminals have been doing," said Borg. "They need to start worrying about what grown-ups could do." Some potential attacks may include shutting down computer systems for several days, changing specifications at automobile plants that may cause cars to explode, and tampering with medical data. The CCU uses its resources to figure out how technology can be used to harm the United States by holding cybersecurity classes for US companies, and investigating attacks on computer systems. After consulting with banks, manufacturers, and other industries, the CCU created a security checklist for companies that identifies 16 potential methods of attack.

'Mashup' Websites Are a Hacker's Dream Come True
New Scientist (05/13/06) Vol. 190, No. 2551, P. 28; P. Marks

The proliferation of mashup sites could present a major security threat, warned some participants at last month's Computer-Human Interaction conference in Montreal, Canada. Mashups, or Web applications that combine information from two or more sites, are often hastily thrown together with no guarantees of accuracy, and privacy and security concerns are sometimes just an afterthought. Mashups have become very popular for the local information they provide--neighborhood crime data overlaid on a Google map, for instance--but there is nothing to stop people from using them to collect addresses or other sensitive identifying information. Mashups have appeared that help commuters monitor traffic and travelers map their journeys, and new mashup sites are appearing at the rate of 10 a week. Google, Microsoft, and Yahoo! have all made the application programming interface (API) of their mapping sites freely available, recognizing that mashup sites help broaden the footprint of their service. But mashup creators do not take the precautions to address concerns such as data integrity, system security, and privacy, according to H. Rossman of Science Applications International. "How do you know the data is real?" Rossman asks. The owners of the sites from which mashup creators pull their data neither know nor care that their information is being used, and the absence of encrypted ID certificates in the exchange between the mashup creator and the source invites the possibility that the data could be coming from a spoofed site, Rossman warns. Mashup sites also do not have rules governing how people's personal information can be used, and viruses could be specifically written to attack mashup sites. A mashup worm could follow the data back to its origin and corrupt its contents, says Rossman. The mounting security concerns come as some mashups, particularly in the travel sector, are growing into huge, multi-million-dollar ventures that play an increasingly important role in people's daily lives.

Voice Encryption May Draw U.S. Scrutiny
New York Times (05/22/06) P. C11; J. Markoff

The FCC, in trying to force Internet and VoIP service providers to adopt technology that will enable law enforcement to monitor phone calls, has left a backdoor open encryption programs that operate directly between computers and not through a hub. Walking through that door is Philip Zimmermann, creator in 1991 of Pretty Good Privacy, software used to encrypt and decrypt email that drew government scrutiny for possible violations of export restrictions on cryptography technology, and more recently Zfone, which encrypts computer-to-computer phone conversations. Unlike similar technology, Zfone performs decryption within the digital voice channel as the call is set up rather than leaving the decryption key residing on a network of computers. For now, the technology does not violate any US regulations due to this difference, but in England, where the government wants to give law enforcement the power

to force businesses and individuals to disclose encryption keys, the issue is not so clear. Z-fone works on free VoIP software programs such as X-Lite and Gizmo but not on Skype calls, which German officials recently announced they can now intercept and decrypt. Zimmerman's software is downloadable for free for now though its creator hopes one day to license it to VoIP software and hardware developers.

Researchers: Spend to Protect Against One Attack, Not Many
IDG News Service (05/19/06), J. Kirk

In a scholarly paper to be presented in June at England's University of Cambridge, a research team from Florida Atlantic University will make a strong and somewhat unusual mathematical case for how companies should spend their IT budgets. The researchers studied how firms can assess their vulnerabilities, determine the risk, and figure out the damage potential. The paper places threats into two categories: distributed attacks, which appear in the form of viruses, spyware, and spam, and focused attacks by a hacker. What the researchers determined, through risk analysis and equations, goes against apparently intuitive computer security efforts. Instead of spending evenly to protect against all attacks, it is not automatically the correct approach if one type of breach could create numerous times more harm than another type. While the "eggs in one basket" effort may worry IT administrators, the research paper reveals that with restricted budgets, compiling defenses against one attack may be the smartest way, as focused attacks have typically proven to create more economic damage than distributed attacks. "We're proposing that companies should look at vulnerabilities of a system, and if they are in high-vulnerability and high-loss scenario, they really, really should spend the most money on targeted attacks trying to prevent hackers," professor Qing Hu said.

Only in America? Copyright Law Key to Global Free Software Model
Linux Insider (05/16/06), H. Meeker

The free software model is seriously threatened by legal systems that lack strong enforcement of copyright law in nations where the development of software is a booming business, writes Greenberg Traurig shareholder H. Meeker. She points to the absence of copyright law enforcement in many emerging nations as a far bigger impediment than the ultimate futility of crafting an international open source license agreement that serves all interests. Even countries that may have some form of copyright protection suffer from lax enforcement policies because of cultural barriers (few Chinese people fluent enough to read English license agreements), governmental barriers (the protection of many Russian piracy outfits from international investigation because they are owned by the military), or judicial corruption (as in India), to name a few reasons. Such nations have flaunted open source software as a cheap alternative that will enable them to adhere to copyright rules while living within their economic means, but Meeker points out that free software has a catch--copyleft. She concludes that a lack of voluntary compliance and enforcement will destroy copyleft, which may cancel its practicality to most of the world. "Ultimately, this may be a question of whether the open source model--as opposed to the free software model--works," Meeker contends. "For what is open source software other than free software without enforcement?"

DHS Privacy Office Bashes RFID Technology to Track People
TechWeb (05/18/06), L. Sullivan

The Dept. of Homeland Security's (DHS) Privacy Office released a draft report that heavily criticizes the privacy and security risks of using radio frequency identification devices

(RFID) for human identification. The technology does not offer a performance benefit for identification purposes compared with other methods, according to the Homeland Department, and could eventually turn the government's identification system into a surveillance system. DHS wants to use RFID to track and locate people across international borders. The report says it is not true that RFID improves the speed of identification. "If RFID is tied to a biometric authentication factor, it can reliably identify human beings; but tying RFID to a biometric authentication negates the speed benefit," according to the report. The committee says DHS' request to track individuals would take away an individual's ability to control when they are identified. The committee suggests that if DHS wants to use RFID technology, individuals should be allowed to turn off signals associated with tracking them or their activities, use of RFID should be limited, and any RFID databases should not be connected to the Internet.