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

Δελτίο 153
15 Ιούλη 2009

Chinese Delay Plan for Censor Software
Wall Street Journal (07/01/09) P. A1; L. Chao; J. Dean; B. Lin

The Chinese government has postponed its mandate that manufacturers embed Web-filtering software in all new PCs sold in the country, in the wake of fervent opposition inside and outside China. The Xinhua news agency quoted a Ministry of Industry and Information Technology representative as saying that some PC makers claimed they did not have sufficient time to meet the July 1 deadline, in which case a delay was permissible. The postponement alleviates global PC companies' worries that complying with the rules would make them susceptible to legal liability and allegations of aiding censorship, yet they also were reluctant to openly challenge China's government, given the heavy concentration of both PC production and PC sales in the country. The Chinese government has said the purpose of implementing the Web-filtering software is to prevent youngsters from viewing online pornography and other "harmful content," and it insists that the software "definitely has no capability for collecting users' information or monitoring their Internet behavior." Information Technology Industry Council (ITIC) president D. Garfield says the computer industry is in favor of enabling parents to block access to objectionable online material, but is against any requirement that specifies a particular company's product. I. Mao with Harvard University's Berkman Center for Internet & Society says the Chinese initiative "has lost legitimacy" and that the government's enforcement of the rule would be impossible. There also are indications that the plan has broadened public interest in China regarding questions about government inquisitiveness and censorship. The postponement does not signal the end of the issue, and a Hewlett-Packard representative said the company is collaborating with the ITIC "to seek additional information, clarify open questions, and monitor developments on this matter."

Cybersecurity Plan to Involve NSA, Telecoms
The Washington Post (07/03/09) P. A1; E. Nakashima; S. Hsu; C. Johnson

Current and former government officials say the Obama administration's cybersecurity plan will involve the US National Security Agency (NSA) and telecom firms. Under the plan, a Bush-era program called Einstein 3 would employ NSA data and hardware to shield the networks of some civilian government agencies, while telecom firms would direct the Internet traffic of civilian agencies through a monitoring box that would seek out and hinder computer codes designed to intrude upon or otherwise compromise networks. The program's purpose is to validate that telecom firms can route only traffic destined for federal civilian agencies via the monitoring system, and to test the technology's effective performance on civilian government networks. The Obama administration is currently considering what components of Einstein 3 to retain, according to former government officials. Experts say the best methods for protecting US computer networks require the automated investigation of email and other electronic communications content, which is already facilitated by commercial providers. Advocates of government involvement say such initiatives should tap the NSA's resources, particularly its database of computer codes that have been connected to cyberattacks or known foes. Sources say the classified NSA system is capable of deciding how to handle malicious incursions, while the program's database also would contain feeds from commercial

firms and the DHS' US Computer Emergency Readiness Team. However, potential NSA involvement is fomenting concern about unwarranted government surveillance of private communication, with former government official S. Baker noting that "the bitter battles over privacy and NSA's role in domestic wiretapping hang over cybersecurity like a toxic cloud."

US Takes Aim at Cyberwarfare
The Washington Times (07/02/09) P. B1; Waterman, Shaun

The US Pentagon's decision last week to open a cybercommand for both offensive and defensive cyberwarfare activities raises a host of questions. US Defense Secretary R. Gates issued a memo to military leaders ordering the Strategic Air Command to have the cybercommand up and running by October 2010, and also assigning Pentagon policy chief M. Flournoy to head a "review of policy and strategy to develop a comprehensive approach to [Dept. of Defense] cyberspace operations." At a recent talk, Deputy Defense Secretary W. Lynn III asked how cyberattacks can be deterred and prevented if it is so difficult to identify adversaries in cyberspace, while Internet Storm Center director Marcus Sachs questioned how rules that apply to real-world warfare, such as the Geneva Convention, can be extended to cyberspace. He also stressed that these issues need to be debated publicly, not privately. Gates' memo urged an "implementation plan" for setting up the cybercommand that would "delineate [its] mission, roles and responsibilities" and its "command and control, reporting and support relationships with combatant commands, [military] services and US government department and agencies." Sachs inquired as to whether the long-term strategy is to have the command concentrate exclusively on military networks, or to cover the entire US critical infrastructure. Lynn implied that the Homeland Security Department would continue to be responsible for the defense of federal civilian networks, while the private sector would watch its own networks. The cybercommand will be placed under the authority of the National Security Agency director. The SANS Institute's A. Paller said that civilian defense against cyberattacks is hampered by civilians' lack of access to the military's latest, best information about attackers and their methods.

Weakness in Social Security Numbers Is Found
The New York Times (07/06/09), J. Markoff

Carnegie Mellon University researchers have demonstrated that Social Security numbers (SSN) can be predicted based solely on an individual's date and location of birth using statistical techniques. They describe their research in the Proceedings of the National Academy of Sciences as "an unexpected consequence of the interaction between multiple data sources, trends in information exposure, and antifraud policy initiatives with unintended effects." The discovery makes the US Social Security numbering system vulnerable to fraud, with the researchers noting that it is now possible to regularly reconstruct sensitive personal information from the kind of online postings often found on social networking sites and other online sources. The researchers used an algorithm on 500,000 publicly available records in the Social Security Administration's Death Master File to successfully identify statistical patterns that then allowed extrapolation to the living US population, making it possible to identify millions of SSNs for individuals whose birth date and location were a matter of public record. The researchers' sample showed that it was possible to identify in a single attempt the first five digits for 44% of deceased individuals who were born after 1988 and for 7% of those born from 1973 to 1988, while the identification of all nine digits for 8.5% of those born after 1988 was possible in less than 1,000 tries. The prediction system's accuracy rose for smaller states and for individuals born after 1988 on account of rules that led increasingly to the de-

signation of Social Security numbers at birth. M. Lassiter with the Social Security Administration has downplayed the significance of the researchers' conclusions, calling their findings "an exaggeration."

Twente Researcher Develops Self-Learning Security System for Computer Networks
University of Twente (07/01/09), J. Bruysters

University of Twente researcher D. Bolzoni has developed SilentDefense, an anomaly network intrusion detection system that could lead to a new generation of network security systems. There are two types of network intrusion detection systems. The first uses a database of all known attacks to identify signatures of commonly used methods, but these systems have difficulty stopping new attack methods. The second uses anomaly detection, essentially learning how the network is normally used and searching for any deviation from the standard pattern. Bolzoni says anomaly detection is not widely used because truly effective systems are not commercially available, but he says SilentDefense will rectify this shortcoming. SilentDefense is based on self-learning algorithms, which significantly improves the accuracy of the system and reduces the odds of false positives. Bolzoni says the ideal network intrusion detection system is not one type or another but a combination of the two. However, before such a system can be created, he says a better anomaly detection system needs to be developed.

Building a Crash-Proof Internet
New Scientist (06/29/09), B. Davis

The Internet's susceptibility to earthquakes, accidents, and other disruptions appears to be greater than people originally assumed, and a great deal of the Net's physical infrastructure is badly outdated, with upgrading challenged by high costs and technical obstacles. Stanford University computer scientist N. McKeown has identified the router as the key to making the Internet more resilient, and with colleague G. Parulkar is working on a system that can modify a router's control software on the spur of the moment while also providing a safe testbed. McKeown hopes that the adoption of the OpenFlow system will allow the Internet to adapt to shifting loads, dynamically tweaking routes to contend with increases in traffic, and making the ride smoother for Web surfers regardless of disruptions. OpenFlow also could facilitate the inexpensive and rapid implementation of a virtual Internet in which thousands of researchers can test and refine novel concepts concurrently. OpenFlow enables software engineers and developers to create their own routes for data packets by writing the algorithms on a regular computer and transmitting them through a secure link to the router, thus allowing the partitioning of a network into any number of isolated sections where researchers can experiment with their ideas. The deployment of new ideas should be accelerated thanks to the open source nature of OpenFlow's software, McKeown says. One of OpenFlow's key advantages could lie in its ability to change the way that data packets travel across the network, as the system could enable competing multipath schemes to be tested on the same network to qualify the benefits they offer. The system also could allow network operators to alter their router's rules so that specific kinds of data are transmitted along specific routes, while network security could be enhanced by OpenFlow because it could enable the testing of more secure versions of router code on existing systems without impeding traffic.

South Korean Web Sites Are Hobbled in New Round of Attacks
The Washington Post (07/10/09) P. A14; B. Harden

Several government, banking, and media Web sites in South Korea were attacked on July 9 in the third wave of a distributed denial of service attack that has targeted sites in that country and the United States since early July. The most recent attack began early Thursday evening, when the MyDoom virus that hackers had planted in thousands of personal and business computers ordered the machines to begin attacking sites belonging to South Korea's Defense Ministry, Foreign Ministry, and parliament, among others. During the attack, the sites slowed down or temporarily stopped working. According to South Korea's National Intelligence Service, the level of the attacks was extremely organized and well planned. The agency said this could mean the attacks were the work of "certain organizations or state." Meanwhile, the attackers seem to have stopped targeting US-based sites. FireEye's A. Lanstein says the attackers removed US government and commercial Web sites from their list of targeted sites on July 7 after those sites began filtering and blocking attack traffic. Experts say the MyDoom virus, which first surfaced in 2004, has been frequently reprogrammed to target new sites. "This wasn't a computer program thrown out into the wild," says CloudShield's P. Jungck. "Someone was actively monitoring its success and changing the targets based on the response. There's a human on the other side playing chess with us."

Researchers Help Set Security Standards for the Internet
Dartmouth News (07/07/09), S. Knapp

Dartmouth College researchers who pioneered the Public Key Infrastructure (PKI) have assumed leadership roles in the establishment of Internet security standards and guidelines. "PKI labors under the misconception that it's difficult," notes Dartmouth PKI architect S. Rea. "PKI is most successful when it runs under the covers or in the background." The US Dept. of Homeland Security is funding a program at Dartmouth's Institute for Security, Technology and Society (ISTS) that seeks to improve the user-friendliness of PKI. The PKI Resource Query Protocol (PRQP) is one of the fruits of this program. ISTS research fellow M. Pala says PRQP delivers a more distributed system for PKI, and obtains genuine references in order to validate the PKI certificates of servers or individuals. Rea and Pala point to the increasing adoption of PKI and an intentional initiative to persuade more and more organizations to embrace PKI with the creation of consortiums organized around common themes and bridge groups combined into a federation to trust everyone within these networks. ISTS research director D. Anthony envisions Dartmouth playing a mentoring or parenting role for PKI and PRQP. "Our students, grad students, and post-docs have learned about this emerging technology since it was born," she says. "And we continue to be involved as PKI and PRQP go global and become the standard way to deploy interoperable computing security."

The Next Hacking Frontier: Your Brain?
Wired News (07/09/09), H. Leggett

Some scientists are concerned that as brain-computer interfaces become widely used and incorporate wireless technologies, "brain hacking" could become a reality. "Neural devices are innovating at an extremely rapid rate and hold tremendous promise for the future," says University of Washington computer security expert T. Kohno. "But if we don't start paying attention to security, we're worried that we might find ourselves in five or 10 years saying we've made a big mistake." Kohno and his colleagues say most devices currently carry few security risks, but as neural engineering becomes more complex and widespread, the potential for serious security breaches expands significantly. For example, the next generation of implantable devices used to control prosthetic limbs will likely include wireless controls that enable physicians to remotely adjust settings. If hackers were to access this system they could take

over a robotic limb. There is a precedent for using computers to cause neurological harm, including the November 2007 and March 2008 hacks of epilepsy support Web sites in which malicious programmers added flashing animations to cause seizures in photo-sensitive patients. Patients also may want to hack their own devices. For example, hacking deep brain stimulators, which already use wireless signals, could enable patients to "self-prescribe" elevated moods or pain relief, which is similar to abusing traditional medications.

IBM Security Software Masks Confidential Info
Network World (07/09/09), M. Cooney

IBM researchers have developed Masking Gateway for Enterprises (MAGEN), software that uses optical character recognition and screen scraping technology to identify and conceal confidential information. IBM says MAGEN can prevent data leakage and allow for data sharing while protecting sensitive business data. MAGEN works at the screen level by "catching" the information before it reaches the screen, analyzing the content, and masking sensitive details that should be hidden from the potential viewer. The system treats the information as a picture, uses optical character recognition to identify confidential sections, and places a data "mask" over those details, without copying, changing, or processing the data. IBM says customers can set masking rules that can be defined per screen structure or per application. MAGEN does not change the software program or data, but rather filters information before it reaches the screen. The software also does not force companies to create modified copies of electronic records to mask, scramble, or eliminate data. IBM says MAGEN could be used for healthcare firms that outsource customer service and claims processing functions to a third party, enabling customer service representatives to access patient records while protecting private medical information.