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

Δελτίο 153
30 Ιούνη 2009

Iran's Web Spying Aided By Western Technology
Wall Street Journal (06/22/09) P. A1; C. Rhoads; L. Chao

Iran has developed a sophisticated system for monitoring and censoring the use of the Internet by its citizens, enabling it to examine and control the content of individual online communications on a wide scale. Technology experts both inside and outside Iran say the country's efforts to monitor Internet information far surpasses blocking access to Web sites or cutting Internet connections. The ongoing political turmoil has shown that Iran has the ability to perform deep-packet inspections, which enables government authorities to block communications, monitor and gather information on individuals, and alter communications for disinformation purposes. The "monitoring center," installed within the Iranian government's telecom monopoly, was part of a larger contract between Iran and a joint venture that included mobile-phone networking technology, says B. Roome, a spokesman for the joint venture, which includes Siemens and Nokia. "If you sell networks, you also, intrinsically, sell the capability to intercept any communication that runs over them," Roome says. In recent months, the Iranian government has experimented with the monitoring technology, but had not used it extensively until the recent unrest. "We didn't know they could do this much," says a network engineer in Tehran. "Now we know they have powerful things that allow them to do very complex tracking on the network." Networking engineers familiar with the system say Iran can control all online communications from a single chokepoint, where emails and social-networking sites are monitored for keywords.

Cell Phones That Listen and Learn
Technology Review (06/22/09), K. Grifantini

A cell phone would be able to track the behavior of its user with SoundSense, new software developed by Dartmouth College researchers. SoundSense automatically classifies sounds as "voice," "music," or "ambient noise," but the user also can train it to recognize unfamiliar sounds. When a sound is frequently picked up via the microphone on a cell phone, SoundSense gives it a high "sound rank" and asks the user whether it is significant and if he or she wants to label the sound. In tests, the software correctly determined when the user was in a particular coffee shop, walking outside, brushing her teeth, cycling, and driving a car. "The SoundSense system is our first step in building a system that can learn [user behavior] on the go," says project leader and Dartmouth professor T. Choudhury. Monitoring everyday sounds via cell phones has the potential to provide people with much information on their daily activities, which could be used to improve their personal healthcare needs or time-management skills. SoundSense does not use a lot of power, sends data elsewhere for processing, stores raw audio clips, and can be told to ignore certain sounds.

NTSB to Look at Possible Computer Role in D.C. Crash
Computerworld (06/23/09), P. Thibodeau

The US National Transportation Safety Board (NTSB) will explore whether computer systems, sensors, or cell phones contributed to the deadly Washington, DC, Metrorail accident

on June 22 in which 9 people were killed. Although there are several other possible reasons for why the Washington Metropolitan Area Transit Authority (WMATA) train crashed into the rear of another train, the WMATA computer systems will likely be closely examined because they are designed to prevent such rear-end accidents. The computer systems are constantly making decisions on train speed using data from track-bed sensors that monitor train movement. NTSB investigators will likely try to rule out possible causes, such as a misconfigured control system, a physical computer or hardware failure, or a security breach, says consultant K. Kawano. Security breaches have been known to happen in transportation systems, and Kawano says he is aware of 10 security incidents in transit systems since 2003. For example, a Polish teen allegedly derailed a train by hacking the network, and in 2003 a widespread worm affected systems used by rail hauler CSX Corp., causing the company to stop some passenger and freight service. Kawano says the design of rail automation systems is so unique that hackers often cannot figure out how to access them. NTSB investigator D. Hersman also says the agency will examine the actions of onboard operators and investigate the possibility of a mechanical failure.

House S&T Committee Discusses Cyberspace Policy Review Report With Federal Agencies, Computing Research Association (06/19/09), N. Gandomi

The US House Science and Technology Committee recently held a hearing to review responses from the Dept. of Homeland Security, the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), and the Defense Advanced Research Projects Agency in regards to the Obama administration's recently released Cyberspace Policy Review report. The report presents several near- and mid-term actions that involve federal agency efforts in research and development, education, standards, information coordination, and interagency collaboration. Technology and Innovation Subcommittee chairman D. Wu (D-Ore.) said previous federal cybersecurity efforts were too "output oriented" and not "outcome driven," and was hopeful that the new administration will focus on achieving fewer breaches of federal systems, reducing incidents of identity theft, and ensuring the security of smart grid systems and health IT systems. Research and Science Education Subcommittee chairman D. Lipinski (D-Ill.) argued for greater collaboration between public and private sectors to expose weaknesses in security and share breach information, and for a multidiscciplinary approach to cybersecurity to provide a better understanding of how people interact with computers and information. C. Furlani, director of NIST's Information Technology Laboratory, said NIST will work with federal, state, local, private, and academic institutions to develop information security standards. J. Wing, assistant director of NSF's Directorate for Computer & Information Science & Engineering, called for increased cybersecurity research openness and more collaborative research between industry and academia.

IBM Claims Privacy Breakthrough for Cloud, Data
InternetNews.com (06/25/09), A. Goldman

A lattice approach could be used to develop fully homomorphic encryption solutions, says IBM researcher C. Gentry, a Stanford University Ph.D. candidate. Gentry's research, which was recently published in the Proceedings of the 2009 ACM International Symposium on Theory of Computing, describes the technique as using an encryption scheme that can evaluate its decryption circuit. A fully homomorphic encryption system could potentially offer unlimited mathematical operations for analyzing encrypted information, compared with the limited operations of normal lattice encoding. Such operations conducted on encrypted text would be more efficient and affordable. Data security, cloud computing, and antispam efforts

all stand to benefit from the ability to manipulate data while leaving it encrypted. "This is ... one of the most remarkable crypto papers ever," says PGP cryptographer H. Finney. "I have to go back to Godel's and Turing's work to think of a comparable example."

Iranian Protesters Avoid Censorship With Navy Technology
Washington Times (06/26/09), E. Lake

Some Iranian protestors dissatisfied with their government's response to the disputed election are using The Onion Router (TOR), an Internet encryption program originally developed by the US Navy, to bypass Iran's censorship efforts. Designed 10 years ago as a way to secure Internet communications between ships at sea, TOR has become an important proxy for Iranians looking to access blocked Web sites. The system of proxy servers that disguise a user's Internet traffic is currently run by the nonprofit Tor Project, which says that TOR connections have jumped 600% since the mass protests in Iran started following the election. Iran, with more than 20 million Internet users out of a population of 70 million people, has a well developed blogosphere. TOR has enabled Iranians to visit government-banned Web sites and avoid detection by the authorities. The Tor Project provides the service by routing Web requests through several different computer servers around the world. While other proxy servers are available, TOR is considered the best because it is an encrypted network of multiple nodes, with each node unlocking encryption to the next node. Wired.com editor N. Shachtman says TOR is different from other methods of evading Internet censorship because it is "all but impossible for governments to track Web sites a TOR user is visiting. TOR is a great way to give Ahmadinejad's Web censors headaches."

Community Colleges Mobilize to Train Cybersecurity Workers
Chronicle of Higher Education (06/26/09) Vol. 55, No. 40, P. A17; M. Parry

Some experts project that the Obama administration's cybersecurity push will expand two-year colleges' role in supplying cybersecurity workers to government agencies, but among the challenges they must overcome is the struggle to train and hold onto qualified cybersecurity educators. Obama's proposed 2010 budget includes $64 million in funding for the National Science Foundation's (NSF's) Advanced Technological Education program, whose projects include the establishment of a platform for cybersecurity education at community colleges. "The time is really ripe for community colleges' role in this area of technology to expand, be recognized, to get the kind of support that it needs," says NSF program director Corby Hovis. "All of the stars, I think, are aligned for this." Colleges are offering cybersecurity courses in anticipation that digital forensics and other cyberdefense areas will be a major source of future career opportunities. The NSF-supported CyberWatch consortium was established to build up the information-security workforce, and most of CyberWatch's 27 member colleges offer degree programs in technical assurance. One CyberWatch member, Anne Arundel Community College, developed a curriculum with National Security Agency representatives and other advisers that has been partially or completely adopted by nine colleges in the Washington, DC, area. Consultant D. Wolf has advised companies to look to community college students for their cybersecurity needs, but University of Tulsa computer scientist S. Shenoi says most community college cybersecurity education programs leave a lot to be desired.

Scars, Marks, and Tattoos: A Soft Biometric for Identifying Suspects and Victims
SPIE (06/15/09), A. Jain; J.-E. Lee

A variety of biometric systems capable of matching fingerprints, faces, and irises are already in use by law enforcement agencies to identify suspects and victims. However, there are numerous situations in which primary biometric traits are either unavailable, are difficult to capture, or where the quality of the image is too poor. In such situations, "soft" biometric traits such as height, sex, eye color, ethnicity, scars, marks, and tattoos can help identify a person. Tattoo patterns are regularly cataloged when booking suspects. Based on an ANSI/-NIST-ITL (Information Technology Laboratory) standard, each image is manually labeled into one of 70 categories and stored with a suspect's criminal history record. Unfortunately, matching tattoos is a time-consuming, subjective process, and the simple class descriptions do not include all the semantic information present in an image. SPIE has developed an automatic tattoo matching system called Tattoo-ID, which uses content-based image retrieval based on tattoo features, such as color, shape, and texture, instead of labels or keywords. Tattoo-ID provides users with a group of images that most closely resemble the queried tattoo. User feedback, based on the retrieved images, can be used to refine feature extraction and the matching capabilities. Tattoo-ID also uses class and subclass labels so users can specify the tattoo image and ANSI/NIST categories, to keep the system compatible with current law enforcement practices.