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

Δελτίο 29
15 Ιουνίου 2006

Pentagon Sets Its Sights on Social Networking Websites
New Scientist (06/10/06), P. Marks

The NSA is funding research into technologies that could extract meaning from the mountains of personal data posted on social networking Web sites. The NSA research could bring the vision of the Semantic Web closer to reality, as it could combine information from social networking sites with other data, such as banking, retail, and property records to create comprehensive profiles of individual users. The focus on social networking sites comes as Americans are still reeling from the revelation that the NSA has been collecting phone call records since shortly after the Sep. 11, 2001, attacks. The NSA plans to conduct similar surveillance of the Web, piecing together a composite picture of individuals by analyzing their contact networks. The Semantic Web will make the comparison of data in disparate formats possible thanks to the common structure known as the Resource Development Framework (RDF). "RDF turns the Web into a kind of universal spreadsheet that is readable by computers as well as people," said D. de Roure, advisor to the W3C. Every piece of numerical data would have its own tag, and different references to the same concept would link to each other. While the Semantic Web is expected to transform Internet search, it will also make it much easier to snoop into people's private lives. Nevertheless, the organization known as the Advanced Research Development Activity, charged with disbursing NSA funds, has taken an active interest in harvesting social networking data to make meaningful connections between people.

Specter Offers Compromise on NSA Surveillance
Washington Post (06/09/06) P. A4; W. Pincus

Sen. A. Specter (R-Pa.) has modified his position on the Bush administration's surveillance programs, proposing legislation that would make the procurement of a warrant from a federal court optional. Specter's move backs away from his earlier stance that the NSA's warrantless surveillance program targeting phone calls and emails of suspected terrorists and associates should be subordinate to the secret court mandated by the Foreign Intelligence Surveillance Act (FISA). The proposal states that it cannot "be construed to limit the constitutional authority of the President to gather foreign intelligence information or monitor the activities and communications of any person reasonably believed to be associated with a foreign enemy of the US." The Bush administration has claimed that its surveillance programs have constitutional authority in their own right, arguing that there is no need for additional legislation. Another provision in Specter's bill would grant immunity to anyone who gave the order for warrantless surveillance under presidential authority. Also, the 29 cases contesting the legality of the NSA program pending in federal courts would be consolidated into a single suit that would ultimately be reviewable by the Supreme Court. Until this point, Specter had been unsuccessful in his attempts to secure an opinion from the administration on a constitutional review of the NSA surveillance program. "I think he [Vice President D. Cheney] is serious about trying to work something out," Specter said. "For the first time, he said they are willing to consider legislation." Sen. D. Feinstein (D-Calif.) said that she cannot support a bill that would authorize government eavesdropping without a court order, and has introduced her own legislation that would only permit government surveillance under the auspices of FISA.

Hacktivists Mount Counter-Offensive to Internet Censorship
IT World Canada (06/08/06), N. Arellano

A group of socially conscious hackers, or "hacktivists," from the University of Toronto has developed software to combat Internet censorship in countries with repressive governments. The software, called Psiphon and developed at the UT Citizen Lab, allows a third-party computer to function as a proxy, enabling Internet users to view restricted content. The Citizen Lab is currently focused on China and other countries that impose censorship, though it is not ignoring Western countries. "Headlines like the Great Firewall of China have spotlighted censorship in that country and others such as Iran and Saudi Arabia, but filtering activities in Western states or so-called democratic countries frequently fly under the radar," said R. Diebert, head of the Citizen Lab. The researchers must act like covert agents in their work as they coordinate with dissidents in repressive countries where discovery is a constant danger. "Identities and locations are kept secret and information is compartmentalized, just as any spy agency would do because in most instances lives are at stake," Diebert said. China maintains an elaborate systems of routers and gateways, using advanced technology to control its citizens' Internet activity. Internet activists in nonrestrictive countries install Psiphon on their computers and create a list of trusted users in repressed countries who can use the computer's IP address to access banned Web sites without being detected. Psiphon encrypts data and travels on a secure network typically used by financial institutions.

Inside the Spyware Scandal
Technology Review (06/06) Vol. 109, No. 2, P. 48; W. Roush

Sony BMG's inclusion of a "rootkit" on their compact discs enabled the company to spy on its customers while giving hackers an exploit through which they could hijack people's computers, and has become symbolic of the increasing distrust media companies seem to be exhibiting toward consumers. This distrust threatens to strangle business as consumers view these companies with equal suspicion. Assessment of the rootkit the record company utilized to conceal copy protection software on CDs--to thwart its location and removal--showed that it could mask other files, such as worms and Trojans, just as easily. Playing the CD on the computer allowed such files to be installed on the computer in secret; and indeed, hackers devised malware to exploit the Sony BMG rootkit shortly after its existence was publicized. The scandal this revelation ignited has re-opened the debate on how consumers should be permitted to use copyrighted digital information, and just how far copyright holders should be allowed to go to protect their intellectual property from unauthorized duplication. "When you build computer systems where you're not protecting the user, but something from the user, you have very bad security," argues Counterpane Internet Security CTO B. Schneier. Princeton University computer scientist J. Halderman alleges that the rootkit's designers must have known that malware writers were familiar with the masking technique they were using. Computer security professionals say the debacle points to the need for digital rights management (DRM) software that is transparent and computer friendly, respectful of users' privacy and security, user serviceable, and above all, flexible.

Wiretap Rules Are Same for Web Calls
Washington Post (06/10/06) P. D1; K. Hart

Internet-based phone services are legally obligated to allow wiretapping by law enforcement officials, the US Court of Appeals for the DC Circuit ruled 2-1 on Friday, upholding an FCC ruling that Web-based phone service providers must follow the same rules as traditional phone companies. However, the court also ruled that private networks such as those at universities and peer-to-peer systems such as instant messaging networks are exempt because they are beyond the law's reach. Making broadband service wiretap-compatible could make such services more expensive, while analysts say more regulation of Web-based phone service is also possible as the FCC may decide that Internet phone companies must pay into the universal telephone service fund. Judge D. Sentelle, writing for the majority, said the FCC "offered a reasonable interpretation" of the law, while Judge H. Edwards in dissent wrote that the law "does not give the FCC unlimited authority to regulate every telecommunications service that might conceivably be used to assist law enforcement." The court's decision may still be appealed. University of Colorado professor P. Weiser says the ruling will force network providers to reengineer their networks, but those costs probably won't be passed down to users. He says, "Any provider of broadband networks now needs to make accounts wiretappable. That's not the way they're engineered and it's certainly not the cheapest way."

Security Onus Is on Developers
eWeek (06/12/06), P. Coffee

At last month's JavaOne Conference, a panel of experts from industry and academia convened to discuss the role of application developers in ensuring software security. Cigital CTO G. McGraw noted the major difference between Java and C from a security standpoint, and that Java cleaned up many of the shortcomings of C. The type-safe Java environment is less prone to bugs, and it provides more cycles to consider security from an architectural standpoint. Regardless of the quality of the individual programmer, mistakes are inevitable, and the most important security considerations revolve around detecting and eliminating the bugs after they occur, said B. Pugh, computer science professor at the University of Maryland. While overall security has improved, software developers are failing to keep pace with the hackers, and some still incorrectly maintain that security is primarily an operating system or a networking problem, according to D. Wagner, professor of computer science at the University of California, Berkeley. When Sun Microsystems co-founder B. Joy first saw the Java-predecessor Oak, he recognized it as an opportunity to develop an environment with a formal semantics where programs are meaningful. Java, Joy notes, is only one layer of an evolving level of higher and higher abstractions required for thorough testing of the high-level properties of a software application.

Brainstorming Ways to Push Open Source
IST Results (06/09/06)

The IST-funded FLOSSPOLS project, which set out to assess the current state of the open-source movement, found that interoperability among different software applications is still lacking. Building on the FLOSS project, which established the world's largest clearinghouse on open-source usage and development, FLOSSPOLS aimed to preserve the European Union's lead in the open-source field. "Our study revealed that preference is often given in business tenders to certain vendors with mostly proprietary software at national and international levels," said project coordinator R. Ghosh. "Whether explicit or implicit, this preference is illegal under EU rules. Hardware preference is already outlawed, yet the use of specific software can often limit competition even more." Ghosh says that even in the absence of major policy support, the rate of open-source adoption in Europe is encouraging, and a program within the European Commission has arrived at a definition for open standards, though it has yet to receive formal approval from the commission. Ghosh is encouraged by the Open Source Observatory, an EC-supported project that serves as a repository for information on open-source deployments by public organizations throughout Europe. In its analysis of gender, the project found that women account for just 2% of participants in open-source development and production, while they make up 20% of general software developers. The project concluded that women face active discrimination, and that European governments need to do more to encourage female participation in the open-source community. The project notes that some companies are more likely to hire developers with open-source skills than applicants with strong university credentials, suggesting that schools should do a better job of partnering with the development community.

Google Researchers Propose TV Eavesdropping
InformationWeek (06/07/06), T. Claburn

Google is in the early R&D stages of developing a scheme that would enable a laptop PC to capture TV sound and immediately deliver personalized Internet content to the computer. Two researchers from the company presented a research paper on the use of ambient-audio identification technology in such a manner last week at the interactive television conference EURO ITV in Athens, Greece. "We showed how to sample the ambient sound emitted from a TV and automatically determine what is being watched from a small signature of the sound--all with complete privacy and minuscule effort," M. Covell and S. Baluja wrote on the Google Research Blog. "The system could keep up with the users while they channel surf, presenting them with a real-time forum about a live political debate one minute and an ad-hoc chat room for a sporting event in the next." Google has not announced any specific product plans for a scheme that could become a promising advertising tool for marketers who want a better understanding of the mass media audience. The company maintains that it takes privacy seriously, and that the system would not be intrusive to the point of intercepting any conversations in the background. Google could ultimately draw more people away from TV and to the Internet if the technology proves to be a success, says analyst C. Brumfield.

Momentum for Global Internet Regulation Mounting
E-Commerce Times (06/08/06), J. Koprowski

The possibility of a global regulatory framework for the Internet will likely be a focus of the next World Summit on the Information Society meeting scheduled for October 30 to November 2 in Athens. The groundwork was already laid at the last WSIS meeting in Tunis with an agreement to establish an Internet Governance Forum under the umbrella of the U.N. aimed at encouraging international participation in Web governance. The author of this article questions how an organization that has proven so inept at doing what it was formed to do initially, keeping peace in the world, could possibly do a good job with governing the Internet, especially considering that the current model seems to be working just fine, with the private sector kicking in any time a problem, such as spam, rears its head. In the end the debate is not about a better Internet but about wresting away its perceived control by U.S. hands. "In many respects, the debate is about who makes the rules, and how the process works," says Thomas Smedinghoff, a partner at the Chicago law firm of Wildman Harrold. "But it's also a debate between those who favor centralized regulation of Internet activities and those who favor a market-driven environment free from intergovernmental oversight and control."

Deploying a Sensor Network in an Extreme Environment
University of Southampton (ECS) (06/11/06), K. Martinez; P. Padhy; A. Elsaify

The GlacsWeb project employs long-lasting wireless sensor nodes implanted under the surface of a glacier, and these nodes employ a totally customized approach to ensure the researchers have direct governance over power management, software, and hardware. The passive sensor probes are encased in plastic and lowered under the ice, feeding data into a low-power base station on top of the deployment site; the base station currently runs embedded Linux and spends most of the time in standby mode. The station uses 500 mW 466 MHz radio modems to transmit the data to a PC at a local cafe, and from there the data is routed to a UK server. The system's performance since deployment reflects the researchers' design decisions and how well they reduce expected risks. The data collected by the system has not only yielded insights on sub-glacial processes, but also on system behavior, such as the communications systems' tendency to be affected by cold and rainy conditions. This year's GlacsWeb deployment will involve a multiple-hop, self-configuring ad-hoc network that would ideally boast fully autonomous and manual-intervention-free probes that offer greater energy efficiency and enhanced data collection. Researchers' direct control of sensor nodes has allowed a multi-agent-based sensor network control protocol to be designed for the project. The researchers say the earlier GlacsWeb deployments and their performance offered clues into refining the system "to be more fault tolerant and 'smarter,'" giving them reason to "believe that the deployments have proved to be essential to a better understanding of how to make real sensor networks."

Trust Me, I'm a Robot
Economist Technology Quarterly (06/06) Vol. 379, No. 8481, P. 18

Important guidelines about the safety and ethical uses of robot technology must be developed as robots migrate from the industrial sector to the consumer arena, according to a new roboethics group that recently gathered in Italy to discuss the issue. Chairman of the Swedish Royal Institute of Technology's European Robotics Network H. Christensen expects the legality of robotic sex dolls resembling children and the admission into households of robots that are strong or heavy enough to crush people to be among the many issues that will gain relevance in the next several years. As robots become more complex, autonomous, and learning-capable, the question of whether their designers should be liable for accidents or malfunctions will become more difficult to answer, notes University of Southern Denmark professor J. Hallam. University of Sussex artificial intelligence expert B. Whitby says efforts to address these concerns are so far insufficient, but there is growing interest among researchers to improve robot safety. The regulation of robot behavior will become more complicated as self-learning mechanisms are incorporated into robotic systems, explains Institute of Intelligent Systems for Automation roboticist G. Veruggio; unpredictable failures will further cloud the issue. Whitby says Asimov's vaunted Three Laws of Robotics will not work because they require the presence of a human-like intelligence to operate, which is beyond the capabilities of robots today. IRobot's C. Angle doubts that learning-capable, general-purpose robots will grow pervasive, and instead expects relatively dumb machines designed for specific chores to become the norm.