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

Δελτίο 149
24 Μάη 2009

EC Wants Software Makers Held Liable for Code
ZDNet UK (05/08/09), T. Espiner

The European Commission is proposing that the European Union's consumer protections for physical products also cover software. Commissioners V. Reding and M. Kuneva say making software companies responsible for the security and efficacy of their products would ultimately improve consumer choice. "If we want consumers to shop around and exploit the potential of digital communications, then we need to give them confidence that their rights are guaranteed," Kuneva says. "That means putting in place and enforcing clear consumer rights that meet the high standards already existing in the main street." The Business Software Alliance's F. Mingorance says the proposed regulatory extension would guarantee all software, including both proprietary and open-source software and beta products, for two years. Mingorance says that forcing software makers to guarantee their products for two years would limit consumer choice. He says software is different from tangible products in that its performance depends on its environment, whether the code is updated, whether the software can adapt and be modified, and whether the code is attacked. "Unlike tangible goods, creators of digital content cannot predict with a high degree of certainty both the product's anticipated uses and its potential performance," Mingorance says. "Extending the scope would force the businesses to maintain update services for such contracts beyond the contractual term and ultimately limit the choice of offers." The proposal also could reduce interoperability between software products, he says.

Cadets Trade the Trenches for Firewalls
New York Times (05/11/09) P. A1; C. Kilgannon; N. Cohen

Throughout the US military there is heightened awareness that the threat of a computer attack is just as urgent as a physical attack, and that military units must be trained to counter it. In April, cadets at West Point and other military academies participated in annual cyberwar games in which teams had to set up secure computer networks and defend them against attacks engineered by the National Science Foundation (NSF). Last year, the Army set up the Network Warfare Battalion, which many of the cadets in the cyberwar games hope to be assignned to. Meanwhile, Nellis Air Force base in Nevada is home to the 57th Information Aggressor Squadron, a group of hackers who use the latest offensive software--some of which was developed by NSF cryptologists--to probe military computer networks for chinks in their armor. Only 80 students graduate each year from the Defense Department's cyberwar schools, but the current Pentagon budget proposals seek to boost the number of students cycled through the schools by 400% in the next two years. Defense Secretary R. Gates says the Pentagon is "desperately short of people who have [cyberdefense] capabilities in this area in all the services, and we have to address it." Establishing a secure Internet link is an early priority for military units when they deploy in combat zones or during a domestic emergency.

Does Anti-Piracy Software on Video Games Open Security Risks on Users' Computers
University of Michigan News Service (05/04/09), N. C. Moore

University of Michigan professor A. Halderman wants to research whether the anti-piracy software built into computer games makes computers more vulnerable to hackers. Halderman will ask the US Copyright Office for a three-year exemption from the Digital Millennium Copyright Act (DMCA) to study the question. He says the DMCA prohibits tampering with copy protection, which means researchers could violate the law if they investigate and suggest repairs for any problems, potentially exposing themselves to lawsuits. In 2003, SunnComm Technologies threatened to sue Halderman after he discovered that the company's new digital rights management (DRM) software was defective and easy to bypass. The software was designed to prevent CD owners from copying songs and uploading them to the Internet, but Halderman found that holding down the shift key when inserting the CD prevented the software from running, giving users access to the audio files. In 2005, Halderman and other researchers found that copy-protected music CDs sold by Sony BMG installed software that created major security holes in users' computers. Sony released a patch to fix the problem, but Halderman discovered that the patch created another vulnerability hackers could exploit. If the Copyright Office grants Halderman's request, he plans to study the anti-piracy software on the game Spore, which installs a DRM program called SecuROM, which some users claim disables critical security measures, including firewalls and antivirus software.

Mathematical Advances Strengthen IT Security
European Science Foundation (05/11/09), S. Valleley

A new cryptography approach based on the mathematical theory of elliptic curves is considered a leading candidate to replace the widely used RSA public key security system. Elliptic curves could enable more efficient cryptography and provide an optimum combination of security and processing efficiency. The European Science Foundation (ESF) recently held a workshop to discuss the potential for elliptic curves and other modern techniques of mathematics in cryptography and information technology security. "The impact of the elliptic curve method for integer factorization has played a role in introducing elliptic curves to cryptographers, albeit for attacking the underlying problem on which RSA is based (the difficulty of factoring integers)," says D. Kohel, convenor of the ESF workshop, from the Institut de Mathematiques de Luminy in Marseille, France. Kohel says the advantage of elliptic curve cryptography is its immunity to the specialized attacks that have degraded the strength of RSA, meaning smaller keys can be used to provide the same levels of protection. "In general, the cryptographer has the benefit over the cryptanalyst (the person attacking the cryptosystem) as he or she can select the key size for any desired level of security, provided everyone has the same base of knowledge of best attacks on the underlying cryptosystem," he says.

Tracking Cyberspies Through the Web Wilderness
New York Times (05/12/09) P. D3; J. Markoff

The Internet is rife with cybercriminals and online eavesdroppers, and countering this threat is the job of cybersleuths. One of the key tools in cybersleuths' arsenal is sniffer programs that can sort out and decode scores of common Internet protocols that are used for all kinds of data communications. One such sniffer is Wireshark, a free and easy to use open source software program. Wireshark was used by the University of Toronto's Information Warfare Monitor research team to uncover evidence that the Dalai Lama's office had been compromised by Ghostnet, a surveillance operation that may possibly be run by the Chinese government. The biggest challenge to cyberforensics is the issue of attribution, or determining who precisely is spying, stealing data, or perpetrating other kinds of cybermischief. The Toronto researchers are seeking to address this problem through a fusion methodology in which Internet data is studied in the context of real world occurrences. "We had a really good hunch that in order to understand what was going on in cyberspace we needed to collect two completely different sets of data," says social scientist R. Rohozinski. "On one hand we needed technical data generated from Internet log files," Rohozinski says. "The other component is trying to understand what is going on in cyberspace by interviewing people, and by understanding how institutions work."

World's First Quantum Cryptography Network Developed in China
Chinese Academy of Sciences (05/07/2009)

Researchers at the University of Science and Technology of China say they have developed the first optical quantum cryptography network. The quantum communication system enables three users to speak in real time with telephones, or one user to broadcast to the other two users by using one-time pad encryption. The network makes use of a chained topography to forward secret keys in a hop-by-hop manner along QKD links. As a result, there are no conditions for using one-time pad authentication and encryption for information transmission. The middle node serves as trusted relays and increases the key generation rate to a higher degree. Researcher P. Jianwei adds that his team has extended the key generation distance to 200 kilometers.

A Blueprint to Stop Browser Attacks
Technology Review (05/14/09), E. Naone

University of Illinois at Chicago (UIC) researchers will present a new way of defending against cross-site scripting attacks at the upcoming IEEE Symposium on Security and Privacy. The new defense enables a Web site to control how user-generated content is transmitted to a Web browser, neutralizing cross-site scripting attacks before they reach the end user. White Hat Security founder J. Grossman says cross-site scripting is the most prevalent threat on the Internet, and although newer Web sites are better equipped to defend against these attacks, there are still millions of vulnerabilities on the Internet. The UIC solution involves a layer of software called Blueprint that can be inserted between user-generated pages and the browser. Blueprint is stored on a Web site's servers, reads user-generated HTML, and checks it against a white list of trusted code, removing any potentially harmful scripts and deciding how content should appear in a browser. The software then reformats the information and transmits it to the browser. For example, Blueprint eliminates characters and symbols that are sometimes used to send unauthorized scripting signals to a user's browser. The solution was tested against 94 types of cross-site scripting attacks and successfully prevented every attack. "What we want to do is to take away the ability for the browser's parser to make any script-identification decisions on the untrusted content that is supplied by the Web application," says UIC professor V. Venkatakrishnan.

Is the U.S. Ready for Government-Sponsored Cyberattacks?
Network World (05/12/09), E. Messmer

A recently published report from the National Research Council (NRC) contends that there has to be more public disclosure and informed debate about cyberarms and cyberwarfare. The report draws a comparison between the unchecked proliferation of cyberweapons and the spread of nuclear arms following World War II. The study sees a growing likelihood for a cyberarms race and cites the undisciplined use of cyberweapons being developed by the US and other countries. Also of concern to the NRC is the absence of formal or comprehensive policies for cyberattacks in the national, political, and military arenas. "Programs to develop cyberattack capabilities are classified and dispersed throughout many program elements within the Department of Defense with the result the overall capabilities are not known even among those with the necessary clearances," the report says. "Effective Congressional oversight that goes beyond a few individuals on the relevant committees is also inhibited." The US Strategic Command Joint Combat and Command of Network Warfare is the military's operations point for offensive cyberattack capabilities, but the NRC study indicates that the US Air Force functions as "the main advocate" and wants to obtain a Cyber Control System that can perform automated network disruptions. The report suggests that the US should be ready to discuss the topic of cyberweaponry in various venues and prepare policy. One of the toughest problems for military institutions that monitor the US computer infrastructure for signs of attack is attribution, or pinpointing the originating source of a cyberattack.

Are Your 'Secret Questions' Too Easily Answered?
Technology Review (05/18/09), R. Lemos

The "secret questions" that protect online accounts and passwords may be far less secure than commonly believed, largely because their answers are often far too simple, researchers say. Carnegie Mellon University and Microsoft researchers will present research at the IEEE Symposium on Security and Privacy, which highlights the vulnerabilities of the secret question systems used to secure the password-reset functions to numerous Web sites. In a study involving 130 people, the researchers found that 28% of the people who knew and were trusted by the study's participants could guess the correct answers to the participant's secret questions, and even people not trusted by the participant had a 17% chance of guessing the correct answer. "Secret questions alone are not as secure as we would like our backup authentication to be," says Microsoft researcher S. Schechter. "Nor are they reliable enough that their use alone is sufficient to ensure users can recover their accounts when they forget their passwords." The least-secure questions are simple ones that can be guessed with no existing knowledge of the subject. Schechter says backup-authentication schemes should be reliable and allow only legitimate users to regain access to their accounts. They also should be secure, preventing unauthorized users from gaining access. The study found that secret questions fail on both accounts. "We would eventually like to see these questions go away," Schechter says. "Unfortunately, since we didn't find many questions that were conclusively good, it's hard to recommend simply changing questions."

ICANN: Apply Public Health Response Model to E-Security
IDG News Service (05/18/09), J. Gliddon

Poor public policy is a bigger threat to the Internet than cyberthreats, according to ICANN CEO P. Twomey. Twomey discussed how ICANN can help curb cyberthreats during a speech at the annual AusCERT conference, and suggested that greater government control of the Internet would create more problems. "We need to think about the Internet's fundamental principles of collaboration, coordination, and communication when dealing with cyberthreats," he said. War and espionage are likely to continue during the Internet age, but a response that is more in line with public health concerns than national security is preferable, Twomey said. The industry should accept that pandemics will occur, but should strive for maintaining a clean commons. "The idea is to attack the swamps, not the fever," he said.