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

Δελτίο 78
11 Ιουνίου 2007

China Prepares for First Strike in Electronic War
eWeek (05/30/07), L. Vaas

The US Department of Defense's yearly congressional report warns that the People's Liberation Army (PLA) of China is gearing up for electronic warfare by establishing information warfare units that are creating viruses to lay siege to adversarial computers and networks, while simultaneously implementing strategies to defend its own computer systems and networks and those of its allies. Electronic and infrared decoys, false target generators, and angle reflectors are some of the other electronic countermeasures China is exploiting outside of malware. Internet Security Advisors Group President I. Winkler said China is second only to Russia as the country most capable of cyber-espionage, and maintained that China has vast resources to devote to acquiring "first strike" capability in a cyber-warfare scenario. Breaches of US computer networks have been attributed to Chinese hackers, who Winkler said are successful because of their ability to exploit both their highly methodical analysis of target systems and their victims' inadequate security deployments. The DoD's report was condemned by China foreign ministry representative Jiang Yu, who claimed the study distorts his nation's military strength and expenses "out of ulterior motives." "Each sovereign state has the right and obligation to develop necessary national defense strength to safeguard its national security and territorial integrity," he argued. "It is totally erroneous and invalid for the US report to play up the so-called 'China Threat.'"

IU Informatics Security Experts Draw New Weapon in War of Cyber Crime
Indiana University (06/04/07)

Indiana University School of Informatics researchers professor M. Jakobsson and research associate S. Srikwan have launched www.SecurityCartoon.com, the first cartoon-based approach to understanding the Internet and the risks faced by typical users. "The cartoons we have developed obviously are not a textbook approach, not made for professional journals or geared to an audience of professional researchers," says Srikwan, who was the graphic designer for the site. "We wanted this to be accessible to anyone who uses the Internet ... That's why the cartoon format is perfect--everybody can relate to it." The cartoons address security issues such as phishing, pharming, malware, spoofing, and password protection, and go beyond the traditional educational efforts to instruct what to do and what not to by explaining the reasons behind the rules, which makes the advice easier to understand, according to Srikwan. The Security Cartoon Web site was developed using scientific methods by IU's Center for Applied Cybersecurity Research (CACR) and the Anti-Phishing Group. "We study the algorithms behind fraud, develop new techniques for combating it, and we investigate how people react psychologically to various threats," says Jakobsson. Jakobsson says that an average of about 5% of American adults are victims of identity theft every year, and that the percentage is increasing as phishing techniques become more advanced.

DHS Sets its Cyber R&D Goals
Federal Computer Week (06/04/07) Vol. 21, No. 16, P. 56; B. Robinson

The Deptτ. of Homeland Security (DHS) says that it will fund and develop potentially groundbreaking cybersecurity software rather than waiting for the industry to develop the required tools. An announcement from the DHS' Cyber Security Research and Development Center asks for industry proposals that, within three years, could create commercial technologies that will protect against computer security threats. The DHS published a list of research and development challenges that are considered to be priorities for neutralizing near-term and long-term threats. D. Maughan, program manager for cybersecurity research at DHS' Science and Technology Directorate, said that anyone interested in making a proposal is strongly considered to approach the DHS with their own technology and transition partners already secured. Purdue University professor E. Spafford, a computer security expert and member of the President's Information Technology Advisory Committee, said that there are several worthy areas on the DHS' research agenda, but that the list of research priorities focuses too much on near-term problems instead of larger challenges. "This announcement is not trying to grow the enterprise by looking to what is coming next, at System X problems," Spafford said. "It's really looking more at fixing what problems exist now." Spafford said that all of the areas on the list need additional research, but there are many other research challenges of equal or even greater importance. Spafford, who also chairs ACM's US Public Policy Committee, added that agencies such as the National Science Foundation also support important cybersecurity research, but that they are under-funded, which makes the DHS programs more important.

Internet2 Security Honcho: PCs Need Universal Healthcare
Ars Technica (06/05/07), K. Fisher

Internet2 security programs manager J. Sauver, speaking at the Anti-Phishing Working Group Counter e-Crime Summit, said that government involvement will eventually be necessary to fight the growing threat of botnets. St. Sauver said that although most compromised computers are used for spam and have little threat beyond that of annoyance, those same compromised machines could be used maliciously to host phishing sites, launch malware, pirate software, host child pornography, capture local traffic for passwords and other sensitive information, or even attack businesses and critical infrastructure. Sauver's primary concern is the lack of responsibility. He said that although the government should not have to shoulder the responsibility of fixing the problem, if the government does not, no one else will. "Just as the government has a responsibility to defend its citizens from conventional military threats or from terrorism, and to respond in case of natural disasters or widespread disease, so, too, the time has come for us to recognize that the government has a compelling national interest in the protection of its citizens and businesses online, and in the protection of their networks and systems," Sauver said. "An attack on US networks and systems, whether blatant or insidious, is an attack on the United States as a whole, and properly deserves national attention and response." Sauver's solution is a Cyber Center for Disease Control that would focus on both massive-scale acute emergencies and recurring problems in PC security. Sauver said the Cyber Center would have to provide anonymity to encourage users to report infestations. He also said the US government should establish a cabinet-level federal agency for cybersecurity with offices in all major cities.

File-Sharing Sites Being Subverted for Web Attacks
New Scientist (05/30/07), M. Inman

Security experts have observed a new trend in distributed denial of service (DDoS) attacks, in which criminals use peer-to-peer (P2P) networks to mount Web attacks. Experts noticed

the first such attacks in January 2007. In traditional DDoS attacks, a gang of hijacked PCs are ordered to overwhelm a target with traffic, but in the case of P2P networks, no computers need to be commandeered. Instead, criminals can corrupt a database by posting fake entries that indicate that a popular file can be found at the address targeted for attack. Thousands of PCs will begin requesting the song or TV episode from the target computer, causing the machine to crash under the flood of traffic. Researchers have demonstrated that anyone with experience in programming could hack into the code of BitTorrent, a popular file-sharing network. Though some contend that there are easier methods for instigating similar attacks, others say the issue is important because of the prominence of P2P networks. In addition, P2P attacks are more difficult to track down and defend against than botnet-based DDoS, says R. Miller of Netcraft.

Could U.S. Repel a Cyberattack?
Christian Science Monitor (06/07/07) P. 1; B. Arnoldy; G. Lubold

The two-week cyberattack against Estonia that flooded government Web sites, shut down a bank's online services, and slowed Internet services across the country, provided US defense officials with a real-life example of what could happen if the United States' Web infrastructure was attacked. While Estonia reacted well, experts say the US may be more likely to suffer mass disruptions of banking, telecommunications, and government services due to a lack of coordination, funding, and centralized authority. Protecting the nation from a cyberattack requires extensive coordination between the government and the private sector and expensive research and preparation, but US-CERT, the small group within the Dept. of Homeland Security (DHS) that is responsible for such efforts, is underfunded and holds little authority, experts say. "The part of the US government that has responsibility for this doesn't have the authority to command attention from within other parts of the government, and it doesn't have the money to get the work done that is on its plate," says cybersecurity expert B. Woodcock, who traveled to Estonia to help during the attack. J. Dixon, acting director of the DHS' National Cyber Security Division, which runs US-CERT, says the situation is improving, citing the increased number of incident reports from the private sector and from government agencies reporting suspicious Internet activity, but that a great deal of work is still needed, particularly in developing state-level preparedness efforts and in preparing for a simultaneous attack against several major networks.

Computer Expert Urges Identity Verification Safeguards for Employee Eligibility Systems, AScribe Newswire (06/07/07)

At a Congressional hearing on Thursday focusing on security and privacy issues affecting efforts to verify employee eligibility, P. Neumann, representing ACM's US Public Policy Committee, testified that the systems requiring employers to submit identifying information on current and potential employees, as outlined in pending legislation, contain many risks. Neumann, an ACM Fellow and Principal Scientist in the Computer Science Laboratory at SRI International, urged Congress to develop incentives for operators and employers to maximize the achievement of US immigration laws mandating employee eligibility verification while simultaneously minimizing privacy and security risks to individuals. Employee Eligibility Verification System (EEVS) expansion is tied to several bills in the House and Senate proposing national systems to verify employment eligibility. Neumann said the computer database applications required by these bills are vulnerable and risk exposing the system and the data. Neumann presented a detailed set of recommendations to ensure the verification system is designed, constructed, and operated securely. "These potential pitfalls to security, integrity

and privacy must be anticipated from the beginning and reflected throughout the design, implementation, and operation of the systems planned to implement the EEVS expansion," Neumann said. "We should not expect easy technological answers to inherently difficult problems." Neumann warned that information sent and stored in EEVS would include primary personal identifiers and that any compromise, theft, leak, destruction, or alteration would have severe consequences, including identity theft and impersonation. "Privacy and security are inextricably linked," Neumann said. "One cannot ever guarantee complete privacy, but the difficulties are severely complicated by systems that are not adequately secure."

Designers Pitch 'Wild and Crazy' Ideas at DAC
EE Times (06/06/07), N. Mokhoff

Some encouraging ideas that have not reached the stage of the technical paper were proposed for computer architectures and design methodologies during the "Wild and Crazy Idea" session at this week's Design Automation Conference. Stanford University researcher A. Solomatnikov discussed the prospects of having a chip multiprocessor generator act as a flexible, universal computing platform that goes beyond the microprocessor. Configuration and programming of the flexible computing framework for running applications of a desired performance would be carried out by designers, and would be followed by the system compiling the program and configuration to adapt the original framework to develop a chip for the specific applications. "Thus, the user gets the reduced development costs of using a flexible solution with the efficiency of a custom chip," explained Solomatnikov. Rice University researcher F. Koushanfar said EDA tools could be used to integrate unique identification keys into gate-level circuits as security protocols. "In the near future, the key design dilemma will be providing security solutions that would cover all aspects of the design--from design reuse methodology, to architecture and to implementation," said Koushanfar. Software piracy could be addressed by using secure IDs to make software that only runs on a specific IC. Also, Blaze DFM researcher P. Gupta said line-end shortening (LES) could lead to faster devices, and Columbia University researcher S. Edwards addressed the possibility of a "precision timed" (PRET) machine.

Online Shoppers Will Pay Extra to Protect Privacy, Carnegie Mellon Study Shows
Carnegie Mellon News (06/06/07), B. Spice; A. Watzman

A new Carnegie Mellon University study shows that online consumers are willing to pay more when shopping at an online retailer with an understandable and strong privacy policy. Participants in the study used a Carnegie Mellon search engine called Privacy Finder, which automatically evaluates a Web site's privacy policy and displays the results on a search results page. The study found that people were more likely to buy from online merchants with good privacy policies, as identified by Privacy Finder, and were willing to pay about 60 cents more on a $15 purchase when shopping at a site with a privacy policy they liked. The study, led by L. Cranor, director of the Carnegie Mellon Usable Privacy and Security Lab, is the first to indicate that online consumers are willing to pay a premium to protect their privacy. "People can't act on information that they don't have or can't understand," Cranor says. Privacy Finder is a search engine Cranor and her students developed to address the problem. Privacy Finder uses the Platform for Privacy Preferences (P3P), a technical standard used to create machine-readable privacy policies. Cranor says that about 10% of all Web sites, more than 20% of e-commerce sites, and about one-third of the top 100 most-visited sites use P3P. Privacy Finder automatically reads and evaluates the policies of Web sites that use P3P, and

displays the information as a series of colored squares that indicate if the site's policies match the user's preferences.

New Record for Quantum Cryptography
Technology Review (06/08/07), N. Savage

The dream of secure communications based on quantum cryptography came a little closer to realization when a team of European researchers successfully transmitted a quantum encryption key across a distance of 144 kilometers--a new record--from a laboratory on La Palma in the Canary Islands to an observatory on Tenerife. The scientists used the phenomenon of quantum entanglement, in which two photons are bound together so that they mirror each other's actions, to create the key. A powerful laser beam was focused through a crystal, resulting in the generation of two entangled photons for every photon that was injected into the crystal. One half of each entangled pair was bounced off a mirror to a light detector on La Palma, while the other photon was routed through a lens to be captured by a telescope on Tenerife and transmitted to another detector. If the signal's reach can be extended just slightly, the transmission of quantum-encrypted data around the world via satellite will become feasible. The researchers' work was detailed in the June 3 edition of the online journal Nature Physics. The scientists are members of SECOQC, a European consortium of about 20 groups developing secure quantum communication, and they are planning a test of a secure system in Europe in 2008.

Net Attack
Wall Street Journal (06/05/07), A. Mannes; J. Hendler

University of Maryland Ph.D. student A. Mannes and Rensselaer Polytechnic Institute computer science professor J. Hendler warn that the cyberwarfare era is upon us, as evidenced by numerous incidents that include an assault on six of the 13 "root servers" comprising the Internet's backbone in February. Such attacks threaten the global economy, and signify the pressing need to strengthen the Internet against criminals. The authors note similarities between various politically charged online attacks, such as the defacing or shuttering of prominent Estonian commercial and government Web sites that followed the relocation of a Soviet World War II memorial in April. These disruptions, as well as the strike against the Internet root servers, take the form of Distributed Denial of Service (DDoS) attacks, in which malware is installed on a computer and directed to swamp a targeted system with messages, which can be crippling when such floods are unleashed en masse by large networks known as botnets. DDoS attacks are becoming more frequent because the tools to launch them are easy to acquire and use, and they are difficult to trace given the global scope of botnet networks. Still, breaching a system to pilfer information or launching an assault that targets real-world infrastructure requires a hacker of substantially greater skill, and Mannes and Hendler note that the few publicly disclosed incidents in this vein have been perpetrated by insiders. But although botnets lack the means to technically hamstring the Internet, they are threatening its trustworthiness and openness through the dissemination of malicious software and spam. The authors point out that establishing international standards to address cybercrime while defending civil liberties is a continuing challenge, but even more formidable is coaxing countries to comply with these standards through the implementation and enforcement of anti-cybercrime laws.

Scientists Discuss Use of DNA and Information Technology
Memphis Commercial Appeal (TN) (06/08/07), D. Connolly

The 13th International Conference on DNA Computing, taking place this week at the University of Memphis, featured discussions from computer scientists from around the world on the next generation of computers and medicines. The conference is based around the idea that nature is better at creating complex systems than human beings. DNA computing was created in 1994 at the University of Southern California when computer scientist L. Adleman wrote a paper outlining his efforts to use biological methods to solve the traveling salesman puzzle, which requires finding the shortest route between several cities. Adleman used a complex method utilizing snippets of DNA to solve the problem, and while scientists have concluded that DNA is not the most efficient way to solve mathematical problems, biological elements could still be used in a process called "self-assembly," according to University of Memphis computer science professor and event organizer M. Garzon. He says proteins and other biological items could be combined to create complex, tiny machines. "The holy grail, if you wish, it to build computational devices, intelligent devices, out of DNA molecules and other molecules," Garzon says. Duke University graduate student U. Majumder, who spoke at the conference about her research, says, "What you're doing is copying nature and building stuff from the bottom up."