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

Δελτίο 77
4 Ιουνίου 2007

After Computer Siege in Estonia, War Fears Turn to Cyberspace
New York Times (05/29/07) P. A1; M. Lander; J. Markoff

The relocation of a Russian bronze statue of a World War II-era Soviet soldier from a park to a military graveyard by Estonian officials triggered what some are describing as the first war in cyberspace. A month-long campaign of attacks against Estonia's electronic infrastructure flooded the Web sites of the Parliament, president, and prime minister, several Web sites of daily newspapers were brought down, and the nation's largest bank, Hansabank, was forced to shut down its online banking network. Estonian officials claim an Internet address belonging to an official in the Russian president's administration was involved in the attack, and attack plans were posted on the Internet in Russian-language forums and chat groups. Russia denies any involvement in the attacks, but has not offered to help track down the people Estonia believes may be involved, saying Estonia needs to be careful when making accusations. Estonia is one of the most Internet-dependent countries in the world, as its citizens rely on the Internet to vote, file taxes, and pay for parking and shopping with their cell phones. "It turned out to be a national security situation," says Estonia's minister of defense J. Aaviksoo. "It can effectively be compared to when your ports are shut to sea." L. Viik, a computer science professor and leader in Estonia's high-tech industry, says the attacks should serve as a learning experience. Scientists and researchers, convened by the National Academy of sciences, recently heard testimony from military strategy experts that indicated both China and Russia have offensive information-warfare programs, and the United States is also believed to have developed a cyberwarfare effort.

Computer Scientists Set on Winning the Computer Virus 'Cold War'
University of Wisconsin-Madison (05/24/07)

Computer scientists at the University of Wisconsin-Madison, the University of California-Berkeley, and Carnegie Mellon University have developed the Static Analyzer for Executables (SAFE), software that targets malware based on its behavior. SAFE examines the behavior of a program before running it and compares the behavior to a list of known malware behaviors, such as reading an address book and sending emails. Any program that performs a suspicious behavior is considered malware. Malware programmers can slip by traditional detection programs by creating a unique signature, requiring traditional malware detection programs to download updates at least every week. By examining the behavior rather than the signature, SAFE can detect malware even if it has a unique signature and only requires updates when a virus appears that exhibits a new behavior, creating a proactive defense rather than reactive. University of Wisconsin-Madison associate professor of computer science S. Jha calls SAFE "the next generation in malware detection." Jha and University of Wisconsin graduate student M. Christodorescu started working on SAFE when they tested different variations of four viruses on Norton and McAfee antivirus software. Norton and McAfee were only able to catch the original variation of each virus. SAFE caught all variations. SAFE will be particularly effective against a new type of malware that is designed to change every time it gets sent to another computer, which can create infinite variations of itself.

Noise Keeps Spooks Out of the Loop
New Scientist (05/23/07), J. Palmer

Texas A&M computer engineering professor L. Kish has developed a secure communication system that he says is more secure, more accurate, and can be used over greater distances than quantum cryptography keys. Kish's cipher device uses a property called thermal noise, which is generated by the natural agitation of electrons within a conductor whenever any amount of voltage is passed through it, but varies depending on the resistance of the conductors. The system can be used to send information, or an encryption key, along any wire, including telephone lines and network cable between two users. Each user has a pair of conductors, one produces high resistance, the other low. When both users select the same type of resistor, either a high amount of noise or a low amount of noise will be produced, signaling both to ignore any communication. When the both chose a different type, an intermediate level of thermal noise is produced, allowing messages to be sent. Kish's cipher successfully sent a secure message down a wire 2,000 kilometers long, much farther than the best quantum key distribution (QKD) devices that have been tried so far. Tests show that a signal sent using Kish's device was received with 99.98% accuracy, and only 0.19% of bits are vulnerable to eavesdropping. Kish's system is also more durable and less expensive, as dust, heat, and vibration can damage QKD devices.

Researcher: RSA 1024-Bit Encryption Not Enough
IDG News Service (05/23/07), J. Kirk

A distributed computing project has enabled researchers to factor a 307-digit number into two prime numbers in 11 months. The development, which is comparable in difficulty to cracking a 700-bit RSA encryption key, suggests that encryption for protecting banking and e-commerce transactions will need to be improved within five years, according to A. Lenstra, a cryptology expert at EPFL (Ecole Polytechnique Federale de Lausanne) in Switzerland. The ability to determine the two prime numbers used to create a public key means it would be possible to calculate the private key and decrypt messages. The researchers created special mathematical formulas to calculate the prime numbers as part of a project that used 300 to 400 off-the-shelf laptop and desktop computers at EPFL, the University of Bonn, and Nippon Telegraph and Telephone in Japan. The 1024-bit RSA encryption is largely used for e-commerce, and it will likely take another five to 10 years to calculate prime number components of current RSA 1024-bit public keys, Lenstra says.

Eyeing Unnoticed Security Researchers
SearchSecurity.com (05/23/07), D. Fisher

SearchSecurity.com executive editor D. Fisher cites six individuals whose contributions to the security domain is worth noting. Former @stake and Matasano Security researcher D. Dai Zovi is described by Veracode CTO Chris Wysopal as "one of the top vulnerability researchers out there based on his skill." Zovi's achievements include the Vitriol virtual machine rootkit, which can undermine the Mac OS kernel, and the KARMA wireless client security assessment tool, which can allow users to view the wireless networks any client in range is searching for. Nate Lawson has a reputation among DVD hackers for co-designing Blue-Ray discs' copy protection scheme, and he also designed the first commercial IDS (RealSecure) and Decru's fibre channel encryption appliance; a major focus of Lawson's work is enhancing the security of hardware devices and embedded software. D. Dittrich, a researcher at the University of Washington's Center for Information Assurance and Cybersecurity, is credited with

having possibly more expertise on botnets and the development of distributed attacks than anyone else in the industry, and he is currently engaged in advanced research and forensics work on peer-to-peer malware and the command-and-control systems of immense botnets. UC Berkeley professor V. Paxson is involved in a National Science Foundation-funded project to furnish an early warning system for new worm activity via the monitoring of unallocated IP address space, and he is also involved with DETER, a joint project between multiple universities and SRI International to explore worm behavior and defenses. Stealth malware such as virtual rootkits is Invisible Things Lab founder J. Rutkowska's specialty, and her work on methods for subverting hardware-based RAM acquisition drew many admirers at this year's Black Hat conference. SPI Dynamics research and development engineer B. Hoffman rounds out Fisher's list for innovations such as Jitko, a pure JavaScript tool that can take advantage of weaknesses in cross-site scripting and construct a large-scale botnet that can be used for anything.

RAW Talent Tackles Risk Analysis
Information Sciences Institute (05/29/07)

An Information Sciences Institute (ISI) research team, working with the support of the Dept. of Homeland Security's Center for Risk and Economic Analysis of Terrorism Events (CREATE), is developing a system that will make the process of quantifying risk estimates faster and more consistent. The analytical tool, called the Risk Analysis Workbench (RAW), will eventually be used by all eight Department of Homeland Security research centers, including CREATE. RAW uses artificial intelligence, information sharing, and Web resources to gather and distribute specific data necessary to perform tree analyses of "what-if" risk scenarios in a quick and uniform process. A major element of RAW is ISI's innovations in the systematic structuring of database information and making such information more accessible over the Internet. RAW will be used to create "decision trees" to provide risk analysis when comparing the cost of prevention against the cost of response, for example, to natural disasters, food born disease, or terrorist attacks. CREATE director D. von Winterfeldt, a professor in USC's Viterbi engineering school, performed one such risk assessment during CREATE's first few years, comparing the cost of equipping all airplanes with counter measures for man-portable anti-aircraft rockets against the repercussions of a successful attack. The analysis was praised as a significant achievement, but the intense effort required to perform such an analysis highlighted the need for a faster, more uniform process. RAW will provide an integrated, generalized toolbox designed to be used by risk analysts throughout the United States, providing a standardized but flexible format. RAW is still in development, but will be distributed in July for research testing.

Spammers' Use of AI Only Just Begun
InfoWorld (06/01/07), M. Hines

Image-based spam attacks have emerged as a new front in the battle against spam, but spammers' use of artificial intelligence in such attacks is only the beginning, concludes a new Forrester Research report. Forrester analysts believe that the use of AI in spamming attacks will only grow more sophisticated and argue that the only way to prevent more attacks is to abandon the current tactic of trying to filter out every type of spam that mass-mailers develop and instead stop spam at its source. Forrester analyst C. Wang says spammers are applying the same principles used in CAPTCHA, the challenge-response test found on may online applications that ask users to input characters found in an misshapen and discolored images, to bypass anti-spam programs. "People have devised new filters that use technologies such as opti-

cal character recognition that has curtailed the spread of image spam," Wang says. "Unfortunately, image spam is only one type of AI problem, and spammers have many they will use in the future; this is only the beginning of an arms race." Wang warns that without a major advancement in AI research, there is no possibility of bridging the gap between the number of methods spammers can deploy and anti-spam defenses. One of the methods that spammers are already beginning to utilize involves sending distorted and obfuscated text images, graphic pictures, and audio and video files, all of which can bypass existing image-filtering tools. Wang says that instead of trying to counter each type of spam, customers and technology providers need to focus on catching messages and fundamental properties contained in each variation, such as links to malware sites that are contained in most of spam messages.

Better Face Recognition Software
Technology Review (05/30/07), M. Williams

The results of the Face Recognition Grand Challenge showed that machine recognition of human individuals has improved tenfold since 2002 and a hundredfold since 1995, and today the best face-recognition algorithms are even more accurate than most humans. National Institute of Science and Technology program manager for tests J. Phillips says the improvement in accuracy is due to the development of high-resolution still images, 3D face-recognition algorithms, and the recent availability of 3D sensors, which directly capture information about the shapes of faces. Current recognition software also focuses more on distinctive features of a human face's surface, such as the curves of the eye sockets, nose, and chin, where tissue and bone are most apparent and do not change over time. Carnegie Mellon Robotics Institute research R. Gross says 3D facial recognition can also recognize subjects from different viewing angles, up to 90 degrees, which was a problem before, possibly because most facial recognition technology was used for tasks involving ID cards and face scanners, which use full frontal faces of cooperative subjects under controlled lighting. High-resolution still images have also improved face-recognition technology with detailed skin-texture analysis. Any patch of skin, called a skin print, can be captured as a image, broken into small blocks that algorithms can then measure, recording lines, pores, and actual skin texture. Gross says skin-texture analysis is capable of identifying differences between identical twins, which is impossible using facial-recognition software alone.

New Agency IARPA Develops Spy Tools
Associated Press (05/31/07), K. Shrader

A new US government agency called the Intelligence Advanced Research Project Activity (IARPA) has been established to develop ground-breaking technology for the US's 16 spy agencies. One technology under development is a "cloaking" technology that bends radar around an object, essentially making it undetectable. Others include smaller power sources using nanotechnology and faster code-breaking quantum computers, according to IARPA acting director S. Nixon. IARPA has met with resistance, however, as members of Congress question the need for such a program. IARPA will be modeled after, though significantly smaller than, the Defense Advanced Research Projects Agency, which was created after the Russians launched Sputnik in 1957. Government agencies have had several technology development success stories in the past. The CIA developed lithium-iodine batteries, which are now used in pacemakers, as well as microdot cameras capable of creating images small enough to be hidden in the period at the end of a sentence. Nixon says that IARPA will not have labs and electron microscopes, but will sponsor research at universities, national labs, and other organizations. Nixon notes that IARPA will not be limited to hard sciences, but will also work on

social-science problems such as finding tools for language research or analyzing the habits of other societies, as well as privacy protection.

Internet Governance Forum in November to Address Access, Security Issues, UN Official Says, eGov Monitor (05/24/07)

The second UN Internet Governance Forum, to be held in Rio de Janeiro Nov. 12-15, will concentrate on issues such as access, security, and openness, according to UN officials who attended a May 23 meeting about potential topics for the forum. Around 200 Internet stakeholders participated in the May 23 meeting, and some participants opined that the November forum should focus more on internationalized domain names and other Internet resources, said M. Kummer, executive coordinator of the forum's secretariat. Participants also felt that the November forum should go beyond the scope of the first forum in Athens. N. Desai, the secretary-general's special adviser on Internet governance, said the shape of the forum could evolve in years to come, explaining that "we are experimenting with a multi-stakeholder open-ended process without a fixed membership." Desai announced that India and Egypt would host the 2008 and 2009 forums, respectively.

Read ID, Real Debate
Washington Technology (05/28/07) Vol. 22, No. 9, P. 24; C. Lipowicz

Security professionals, vendors, and trade groups continue to argue over the feasibility and effectiveness of the 2005 Real ID Act, which would standardize driver's licenses nationwide. Under the act, states would gather and electronically house millions of individuals' personal information, and the states' databases would link together. The concept was developed by the 9/11 Commission to close gaps in the current system, but critics contend that the act's mandates would put people at risk for identity theft, racial profiling, and other threats to civil liberties. Eugene Spafford, ACM's US policy committee chairman, asserted that Real ID sets up the possibility of identity theft "on an unprecedented scale," and voiced concerns that states will establish insufficient privacy protections as they hurry to meet Real ID deadlines. Spafford cited audit trails, strong data access controls, and employee background checks as types of protections that should be employed, as well as a paper trail for the system. The DHS Data Privacy and Integrity Advisory Committee declined to sanction the program, as panelists felt that concerns about privacy, data security, and cost, among others, had yet to be resolved. Still, the committee noted that the American Association of Motor Vehicle Administrators' (AAMVA) database system could be a potential prototype for Real ID. ACM also characterized AAMVA's system as "effective," and said that its system design could create a national database, if expanded in scope.