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

Δελτίο 59
1 Φλεβάρη 2007

NIST Announces Competition for New Cryptographic Hash Algorithm
Network World (01/23/07)

Citing recent attacks on the cryptographic hash algorithm currently used to establish digital signatures and authenticate data, the National Institute of Standards and Technology will hold a competition to choose a new algorithm to become the federal information processing standard. The current standards include variations of the Secure Hash Algorithm, SHA-1, SHA-2, SHA-256, SHA-384, and SHA-512. The Advanced Encryption Standard used today was also chosen from a worldwide competition and improved through peer review. "As a first step in this process, NIST is looking for comments on its recently published draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms," said NIST's J. Kosko. According to a NIST statement in the Federal Register, NIST is interested in "unclassified, publicly disclosed" algorithms that are "royalty-free" and "capable of protecting sensitive government information well into the foreseeable future." The statement also said the "draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash functions" will be presented at the RSA Conference in San Francisco. A baseline is planned to be completed by the third quarter of this year, followed by a round of submissions due by the third quarter of 2008. Public comments on the selected candidates would last until the fourth quarter of 2009, at which point NIST will decide whether to extend the proceedings or to enter chosen submissions into public workshops for discussion.

Cyberthreat Experts to Meet at Secretive Conference
CNet (01/22/07), J. Evers

Meetings will be held later this week at Microsoft's Redmond, Wash., headquarters to provide a confidential forum for representatives from security companies, government, and law enforcement to discuss the threats facing the Internet. High on the list of priorities are botnets and the use of zero-day bugs, but many topics will be covered. Trend Micro's D. Otis will give a presentation on email authentication technology named Sender ID, which would be exploited to launch denial-of-service-attacks. Another presentation, given by the Anti-Phishing Workgroup's D. Jevans, will provide an overview of phishing statistics and cover new patterns in data-theft, including subdomains, man-in-the-middle style attacks, and the way attack patterns are changed to target smaller banks and payment services. MessageLabs' A. Shipp will give a presentation on Trojan horses that attack a small number of businesses or individuals. Shipp believes the event will allow for valuable discussion that will make those involved better equipped with deal with security threats: "What are the bad guys doing now and how can we stop them?" he asked. "Can we do better than we are currently or do we need a seismic shift in the way we do things now to solve the problems? What kind of co-operative efforts can we put in place that would benefit us all?" In order to solve the security problem, communication and cooperation within the industry are vital, says Norman Data Defense Systems chief research officer R. Zwienenberg. "Without worldwide laws and cooperation, we might lose the battle in the end," he warns.

The Secret to Secure Code - Stop Repeating Old Mistakes
Between the Lines (Blog) (01/16/07), D. Farber

Though programmers will never be able to put an end to hackers, the Fortify Technical Advisory Board believes they can take a considerable step in the right direction by not repeating their mistakes, and implementing security within products from the ground up. "The industry is currently defaulting to a small number of platforms?Windows, Java and a few others," explains Windows Live China managing director Li Gong. "Once the platform is built it is hard to make it more secure. You only get one or two chances to make it more secure, especially once it ships. Because [of] its layers, you have to solve the security problems at each layer." The board also blames the poor status of security on the lack of security experts in development teams, stressing that simply adding a few security experts is not enough if the rest of the programmers are ignorant of security. "There is the issue of security and the issue of good coding practices," says University of California, Berkeley, computer science professor M. Bishop. "They are interlinked. Everyone has to use best practices--the chain is only as strong as weakest link." Focusing on the idea that security applies to the system as a whole, not just as a single element, the board explained how as layers are improved, hackers are looking to more obscure parts of code to tamper with, as many programmers do not have the time to deal with such seemingly peripheral concerns. A constant need for updated textbooks was also discussed. However, the experts did praise Microsoft as a leader in integrating security measures into its entire development process.

'Storm Worm' Trojan Horse Surges On
CNet (01/22/07), T. Espiner

Security firms are dismayed by the aggressive Trojan horse that was unleashed on computers around the world last weekend. They do not know who is behind the attack, from where it was launched, and are still trying to understand the extent of the botnet associated with the Trojan "Storm Worm." According to antivirus vendor F-Secure, Storm Worm started Friday as an email about storms in Europe, which sought to get recipients to download an executable file to read the news story, and six subsequent attacks over the weekend similarly tried to woo readers with news such as a missile test by China or the death of F. Castro. F-Secure adds that each version of the emails was capable of updating itself, which prevented most antivirus programs from detecting it. "The bad guys are putting a lot of effort into it--they were putting out updates hour after hour," says M. Hypponen, director of antivirus research at F-Secure. The compromised machines, possibly hundreds of thousands of home computers, were turned into zombie machines for a botnet that acted like a peer-to-peer network, in that it has no centralized control. Attackers tend to control botnets through a central server, which can be located, ultimately allowing zombie networks to be taken down and destroyed.

UMass Scientist's Program Combats Hackers
Massachusetts Daily Collegian (01/29/07), M. Osorio

University of Massachusetts computer scientist E. Berger developed anti-hacking software, called DieHard, that takes advantage of the surplus memory and power of today's computers. Hackers often can gain access to sensitive information when programs request less memory than they need, causing information to overflow into other parts of the memory, which Berger compares to houses. The result is an override of these other "houses." Hackers often seek out the "house" that contains a user's sensitive information and add their own information to it in order to cause an override. DieHard acts as a wall between a computer and those trying

to access it through programming deficiencies by using different keys and hiding sensitive information in a safe location. "Every house is the same, the floor plan is the same, the important information is all in the same place and you have keys to the house," said Berger. "That's the symbol of all computers. If you have one key you can rob anyone blind. What DieHard essentially does is to make the key different for every house and stash the valuables in different places." DieHard does cause a 50 to 75 percent increase in memory consumption, but should not make a system noticeably slower. The program works with Linux, Solaris, and Windows systems, and can protect any application in Linux or Solaris, but for now it can only protect Mozilla Firefox on Windows XP and 2003 systems. Berger has received grants from the National Science Foundation, Intel, and Microsoft for her work.

Olde Fashioned Legal Loopholes Allow Rigging of Hi-Tech Elections
VoteTrustUSA (01/30/07), H. Stanislevic; J. Washburn

Elections can be fixed by exploiting legal loopholes in election reform legislation, leading software test professional J. Washburn and computer network engineer H. Stanislevic to conclude that any such legislation should be rated according to its ability and intent to lower the risks of such exploitation. Election management servers (EMS) can be linked to the Internet even though Internet connections may be prohibited for voting machines on which votes are cast, creating a situation in which a Trojan horse program can be introduced or the ballot definition corrupted, facilitating the election of the wrong candidate or the disenfranchisement of voters, among other things. A second loophole allows a high failure rate for equipment while not disqualifying equipment from service. This renders denial of service attacks indistinguishable from "normal" in situ malfunctions that fall under federal standards, once again clearing the way for voter disenfranchisement and the election of the wrong candidate. Instructions that direct voters to confirm voter verifiable records are insufficient or nonexistent, which means the wrong candidate could be elected while discrepancies between the DRE Summary screens and voter certifiable paper records cannot be spotted by voters even in the event of a full recount. A fourth loophole is the lack of a requirement to conduct statistically meaningful audits, which can lead once more to the election of the incorrect candidate. Former ACM President B. Simons thinks Internet access to election management systems is "a very bad idea," and draws a distinction between Internet connections and the display of election data on a Web site, which presents no danger. Washburn and Stanislevic think that "anyone with a bona fide interest in election integrity should be on the lookout for the above loopholes ... in any current or proposed legislation and must fight to close them before it's too late."

A Lively Market, Legal and Not, for Software Bugs
New York Times (01/30/07) P. A1; B. Stone

Both hackers and security companies engage in the buying, selling, and trading of software vulnerabilities, but for a researcher who has discovered a bug, the black market is often more tempting. Companies such as Microsoft encourage security researchers to report bugs rather than sell them, but there is no monetary incentive to do so. "To find a vulnerability, you have to do a lot of hard work," says E. Legerov, founder of a small security firm in Moscow. "If you follow what they call responsible disclosure, in most cases all you receive is an ordinary thank you or sometimes nothing at all." Instead, Legerov's company sells this information directly to corporate customers at prices starting at $10,000 for periodic updates. In the 1990s, a sort of agreement was reached where security researchers would inform software manufacturers of bugs and allow time for them to release official patches before disclosing the flaw to

the public, as long as the manufacturer gave them credit for their discovery. However, this era of researchers who were satisfied by simply being recognized began to erode about five years ago as security companies began to purchase vulnerabilities and provide clients with solutions, claiming that both clients and manufacturers were notified before the public. The criminal marketplace for vulnerabilities, and the high prices it can generate, gained attention in January 2006, when a group of Russian hackers were found to have sold a zero-day program aimed at Windows Metafile (WMF) that led to spyware and malware being planted in tens of thousands of computers worldwide. "You will always make more [money] from [selling vulnerabilities or malicious code to] bad guys than from a company like 3Com," says eEye Digital Security co-founder M. Maiffret.

New York Halts E-Voting Machine Testing
Computerworld (01/29/07), M. Songini

The New York State Board of Elections has suspended the evaluation and certification of e-voting machines because Ciber, the company contracted to do the job, had not met the requirements established in 2005. A Ciber representative says, "The issues found in the audit do not reflect on the accuracy of tests conducted before the audit. Ciber was accredited at the time those tests were conducted, and they met all of the standards set for testing and accreditation at that time." The US Election Assistance Commission (EAC) confirmed that the failure to meet requirements was due to problems in the company's documentation process, although the specific problems were not identified. Ciber had requested a special interim accreditation available to businesses whose applications for 2005 certifications had not yet been processed, but the EAC turned down the request. Ciber has sent a portion of the audit report conducted by the EAC to the New York State Board of Elections for review. The Ciber representative said the issues initially raised in the audit have been addressed and the company is waiting for further notification. However, EAC Executive Director T. Wilkey wrote a letter to Ciber's Wally Birdseye claiming that the company had failed to follow its own quality management requirements. The Ciber representative said "we don't feel it's appropriate to comment further on the [audit] process while it is still underway. Our focus is to concentrate our resources on addressing any issues, completing the process, and achieving accreditation."

FBI Turns to Broad New Wiretap Method
CNet (01/30/07), D. McCullagh

A University of Colorado law professor recently detailed an FBI surveillance technique where electronic information from thousands of users is obtained and placed into a searchable database if a specific individual or their IP address cannot be found. This "full-pipe" surveillance is capable of recording all Internet traffic flowing through a network, with interception occurring inside an IP's network at the junction point of a router or network switch. "You intercept first and you use whatever filtering, data mining to get at the information about the person you're trying to monitor," said P. Ohm, who shed light on the practice at the Search & Seizure in the Digital Age Symposium held at Stanford last week. This new system is being called more invasive than the FBI Carnivore surveillance program, which was abandoned two years ago. Federal law states that the FBI must perform "minimization," whereby agents must "minimize the interception of communications not otherwise subject to interception" and inform the supervising judge as to what is happening. However, another section of the law states that if the information being obtained is in code or a foreign language and no expert in that language is readily available, "minimization may be accomplished as soon as practicable after such interception." Since digital communication is all encoded, investigators

can record as much as they please, without sorting it out until later. In 1978, US v. Pine stated that investigators are allowed to keep listening to a tapped phone line in order to prosecute other illegal activities not originally mentioned in the wiretap order, suggesting that the same could be done with information obtained through full-pipe surveillance.

New UNH Model Measures Cyber Threat
Foster's Daily Democrat (NH) (01/26/07), T. Kressler

Students and researchers of the University of New Hampshire's Justiceworks Technical Analysis Group have developed a computer model that can be used to evaluate the threat of a cyber attack posed by a specific terrorist group, individual, or nation. The Cyber Threat Calculator produces a value indicating the level of threat based on several variables, the two most prominent of which are intent and capability. Actual groups and countries were used as case studies when the Threat Calculator was demonstrated at the Department of Defense cyber crime conference in St. Louis. A friendly but technologically advanced country would have a high variable for their capability to harm the United States, but the threat level would be brought down by their low variable for intent to do harm. The Threat Calculator is designed to evaluate large-scale strategic threats, rather than tactical threats such as viruses, worms, and identity theft. The United States must prepare for attacks on targets such as power grids, emergency response systems, financial services, and telecommunications, says UNH professor, Justiceworks researcher, and contributing research for the Department of Homeland Security A. Macpherson. Justiceworks plans for the Threat Calculator to be on the Web by late summer so any organization can utilize it.

Tech's Dark Potential Troubles Terror Expert
Mercury News (01/29/07), F. Davies

Former US terrorism czar R. Clarke's new book, "Breakpoint," pictures a world at the mercy of cyber terrorism, where biotechnological advancements allow wealthy parents to create ideal children and brain links offer enhancements that could change the very nature of humanity. At a recent book signing, Clarke cited a Chinese general who claimed that "China could turn off the US power grid (through a cyber attack) during a war." Clarke, who said he spoke with futurist R. Kurzweil about the technology discussed in the book, claimed, "Some of these things sound like science fiction, but they're not." He noted the difficulty in projecting when certain technologies will emerge; even if they are banned in the United States, they could be developed elsewhere. "We need to be aware of what's coming, because sometimes new technologies burst on the scene before we decide if we want them and what the consequences are," Clarke said. Nanotechnological and neurological innovations currently allow brain implants to provide hearing to the deaf and allow the paralyzed to move a mouse-like device with their thoughts alone, and the military has already tested brain-computer linkage and worked on exoskeleton body suits. Bioethicist J. Hughes, who admits that "the scenarios Clarke describes are quite plausible," stresses the need to make such technology widely available if it does become a reality, rather than allowing it to be limited to those who can most afford it.