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

Δελτίο 140
30 Γενάρη 2009

Group Details 25 Most Dangerous Coding Errors Hackers Exploit
Computerworld (01/12/09), J. Vijayan

A group of 35 high-profile organizations, including the US Dept. of Homeland Security and the National Security Agency's Information Assurance Division, has released a list of the 25 most serious programming errors. The goal is to focus attention on dangerous software-development practices and ways to avoid those practices, according to officials at the SANS Institute, which coordinated the list's creation. Releasing the list is intended to give software buyers, developers, and training programs a tool to identify programming errors known to create serious security risks. The list will be adjusted as necessary to accommodate new or particularly dangerous programming errors that might arise. The list is divided into three classes. Nine errors on the list are categorized as insecure interactions between components, another nine are classified as risky resource management errors, and the rest are considered "porous defense" problems. The top two problems are improper input validation and improper output encoding errors, which are regularly made by numerous programmers and are believed to be responsible for the attacks that compromised hundreds of thousands of Web pages and databases in 2008. Other programming errors include a failure to preserve SQL query, Web page structures leading to SQL injection attacks, cross-site scripting vulnerabilities, buffer-overflow mistakes, and chatter error messages.

Voting Machine Audit Logs Raise More Questions About Lost Votes in CA Election
Wired News (01/13/09), K. Zetter

Computer audit logs, created by the Global Election Management System (GEMS) tabulation software from Premier Election Solutions, continue to raise questions about how the vote tabulation system lost ballots during the November US election. The logs also raise doubts about the general reliability of voting system audit logs to record the events during an election and ensure the integrity of results. The logs are the focus of an investigation by California's secretary of state to determine why the GEMS tabulation system deleted 197 ballots from the tallies in Humboldt County during the November general election. However, instead of providing transparency into what occurred in the voting system, the GEMS logs have only further perplexed state investigators. Deputy secretary of state Lowell Finley says the logs are a foreign language to anyone other than a programmer, but University of Iowa computer scientist D. Jones says the logs are no clearer to him. Jones says the audit logs could provide some assurances about an election if they were designed so a casual observer could understand them, but instead they are cryptic and obscure, destroying their value in terms of election transparency. The computer audit logs are supposed to track activity on a voting system to help officials investigate problems as they occur and ensure that no one tampers with the software. However, the GEMS logs do not provide a date or time stamp to indicate when events occurred, nor do they record when files are intentionally deleted from the system or unintentionally erased. Premier told state officials that a different log records deletions, but state officials were unable to find evidence of deletions in that log either.

Government Spends Over $30 Million to Sharpen Cyber Security Saber
Network World (01/09/09)

The US Defense Advanced Research Projects Agency recently named the major contractors that will develop the first phase of technologies aimed at dramatically improving cybersecurity as part of the $30 million National Cyber Range program. The projects will test a variety of technologies, including hot security systems that could modify or replace operating systems and kernels; local-area-network security tools and suites that could require modifying or replacing traditional network device operating systems; and new protocols that may replace portions or the entirety of today's protocol stacks. The projects also will research wide-area-network systems that operate on bandwidths currently not available commercially, and tactical networks that may include mobile ad hoc networks or maritime systems. The program's objectives include being able to offer the use of highly advanced test facilities, establishing an administration capable of certifying and accrediting new technology, and managing security and scheduling testing. "Addressing the vulnerabilities within our cyberinfrastructure must become our long-term national security and economic security priority," says US Joint Interagency Cyber Task Force director M. Hathaway. "I don't believe that this is a single-year or even a multi-year investment--it's a multi-decade approach."

DECT Cordless Phones No Longer Secure
Network World Canada (01/07/09), P. Judge; G. Meckbach

Researchers at the 25th Chaos Communications Congress in Berlin, Germany, recently demonstrated that they could eavesdrop on calls made using Digital Enhanced Cordless Telecommunications (DECT) wireless networks. "DECT really ought to be used for consumer applications and avoided by enterprises," says Info-Tech Research Group analyst M. Tauschek. "Get rid of anything that you have that's based on DECT." The attack used a Linux laptop with a modified laptop card that can directly intercept calls and information, recording everything in a digital form. Even if encryption is turned on, the system can bypass it by pretending to be a base station that does not support encryption. A. Schuler, from the Dedected group, which demonstrated the attack, says if someone fakes being an unencrypted base station and DECT devices cannot get encryption to work, all the most popular phones will revert to unencrypted communications as the priority of manufacturers is interoperability not security. University of Luxembourg cryptographer and Dedected member R.-P. Weinmann says it is not clear whether the same method would work on debit card reading systems, since they may enforce the use of encryption or use higher level encryption such as secure sockets layer. Nevertheless, Tauschek says retailers that use wireless point-of-sale terminals should use a different standard that has better security features, such as the Advanced Encryption Standard.

Keeping Information Safe From Digital Spies
Daily Bruin (01/08/09), S. Bui

As people become increasingly dependent on digital technology, security and privacy concerns will be growing issues for the next several decades, says A. Sahai, the associate director of the Center for Information and Computation Security (CICS) at the University of California, Los Angeles (UCLA). UCLA professor J. Palsberg predicts that 2009 will see an increasing number of headline stories on cyberterrorism, against both countries and multinational organizations. "More and more, people will wonder whether the increasing computerization of healthcare will make their most personal data be one cyberattack away from falling into the wrong hands," Palsberg says. "Pundits will call for the Obama administration to pre-

pare the nation better for cyberattacks." Sahai notes that there have been some revolutionary breakthroughs in cybersecurity research in the past decade. CICS is developing new protective technologies, including functional encryption, biomedic-based encryptions, and reliable routing of the Internet. Sahai says functional encryption involves a sophisticated system in which multiple keys provide access to specific data. Artificial intelligence (AI), particularly machine learning, could potentially offer more secure systems that learn to automatically recognize patterns and objects, Sahai says. "In AI, traditionally these programs are usually trying to understand handwriting, or speech, or see objects like people or facial expressions," he says. "But in cybersecurity, some of the same ideas and algorithms can be used to identify viruses or spyware."

US Plots Major Upgrade to Internet Router Security
Network World (01/15/09), C. D. Marsan

The US Dept. of Homeland Security (DHS) plans to quadruple its investment in research dedicated to securing the Border Gateway Protocol (BGP) by adding digital signatures to router communications. DHS says the research initiative, dubbed BGPSEC, will prevent routing hijackings and accidental misconfigurations of routing data. DHS expects BGPSEC to take several years to develop prototypes and standards and at least four years before deployment. Experts have praised the accelerated effort, as BGP is one of the Internet's most vulnerable faults. "The reason BGP problems are so serious is that they attack the Internet infrastructure, rather than particular hosts," says Columbia University professor of computer science S. Bellovin. "This is why it is a DHS-type of problem." Arbor Networks' D. McPherson says BGP is one of the largest threats on the Internet. "There doesn't exist a formally verifiable source for who owns what address space on the Internet, and absent that you can't really validate the routing system," McPherson says. The extra funding should enable the DHS to develop ways of authenticating Internet Protocol (IP) address allocations and router announcements on how to reach blocks of IP addresses. DHS funding for router security will rise to approximately $2.5 million per year beginning this year, up from about $600,000 per year over the last three years, says D. Maughan, DHS program manager for cybersecurity research and development.

Low-Cost Strategy Developed for Curbing Computer Worms
UC Davis News & Information (01/14/09), L. Greensfelder

A new strategy for guarding against computer worms has network computers share data about the probability that an attack is taking place. "One suspicious activity in a network with 100 computers can't tell you much," says S. Cheetancheri, who developed the strategy when he was a graduate student in the Computer Security Laboratory at the University of California, Davis. "But when you see half a dozen activities and counting, you know that something's happening." The strategy uses an algorithm to compare the cost of disconnecting a computer from the network to the cost of having an infected machine, based on the probability of an attack and what the computer is used for. A toggle would be triggered to disconnect a computer if an infection costs more than staying online. For example, a copy writer might be moved offline even if there is a low probability of an attack, but someone in online sales might not be disconnected until it is almost certain that the activity is malicious.

Let the Cracking Begin
Government Computer News (01/12/09), W. Jackson

Analysts have started the process of testing new Secure Hash Algorithm (SHA) candidates for flaws as part of the first round of the National Institute of Standards and Technology's (NIST's) competition to select the next government standard for cryptographic tools. So far, three of the initial 51 submissions have been eliminated. NIST's B. Burr says there are probably more than 3 or 4 more broken algorithms that have not been withdrawn from consideration yet. The winning submission will become SHA-3, and will augment and eventually replace the algorithms currently specified in Federal Information Processing Standard 180-2, which uses SHA-1 and SHA-2. Officials decided to create a competition to design SHA-3 in 2007 after weaknesses were discovered in the existing algorithms. The final selection of a new standard is expected to take place in 2012. Candidates for SHA-3 must be publicly disclosed and available without royalties, work on a wide variety of hardware and software platforms and support 224, 256 and 512-bit encryption. NIST will hold several public workshops to continue to narrow the field, and expects to reduce the number of submissions to 15 by late summer, with the final 5 being selected in 2010.

Rice University Software Helps ID Terrorists Carrying Out Attacks
Rice University (01/12/09), F. Brotzen

Rice University researchers have developed a new computer program that rapidly scans large news report databases to determine which terrorists groups could be responsible for new attacks. The program was used to quickly identify the Pakistan-based Lashkar-e-Tayyiba group as the most likely culprit for the Thanksgiving Day attack in Mumbai. "There's an enormous amount of value in using computing to profile conflicts," says C. Bronk, a member of the software development team. "While experts on conflict are essential, they need new tools for coping with information overload. That’s what we're trying to provide." Bronk says the Rice project demonstrates that technology can be used to determine where to look, enabling human efforts to be more focused for better assessment and analysis. The goal is to perfect a system that can assist the government in identifying future "hot spots" of activity before an attack occurs. On the day of the attacks in Mumbai, Rice undergraduate student Sean Graham ran several queries based on the information reported by TV networks. By entering the weapons used in the attack, the targets, and tactics, with no input on geographic or ideological influence, the program identified several possible culprits. The researchers then focused on groups active in South Asia, which reduced the list of possibilities. When the list of the groups was run against a second database constructed by researchers at the University of Maryland, Lashkar-e-Tayyiba was found to be the most likely perpetrator. "We designed the software to better assign attribution in terror attacks, and it appears to have worked," Bronk says.

Worm Infects Millions of Computers Worldwide
New York Times (01/23/09), J. Markoff

A computer worm is infecting millions of computers in what could be the first part of a multi-stage attack. The worm, known as Conflicker or Downadup, has spread by exploiting a recently discovered Microsoft Windows vulnerability that involves guessing network passwords and using portable devices such as USB to spread. Experts say the worm has led to the worst infection since the Slammer worm in January 2003, and it may have infected as many as 9 million PC worldwide. Many computer users may not notice that their machines have been infected, and computer security researchers say they were waiting for infected computers to receive instructions so they can determine the intended purpose of the botnet. Infected computers may run programs in the background to send spam, infect other computers, or ste-

al personal information. Microsoft released an emergency patch to eliminate the vulnerability in October, but the worm has continued to spread. Security researchers at the Qualys security firm estimate that about 30% of Windows-based computers attached to the Internet remain vulnerable because they have not been updated with the patch. "I don't know why people aren't more afraid of these programs," says Georgia Institute of Technology professor M. Furst. "This is like having a mole in your organization that can do things like send out any information it finds on machines it infects."

Building a Better Spam-Blocking CAPTCHA
Computerworld (01/23/09), S. Vaughan-Nichols

Malware designers and spammers have become increasingly adept at tricking Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) security systems on Web sites. Spammers and crackers have created programs capable of defeating CAPTCHAs, and have released cracking software to enable anyone to beat them. These programs use optical character recognition (OCR) software to sort through a CAPTCHA's squiggly text. If a program fails, it tries again, exploiting the fact that some CAPTCHAs do not present new text to users who fail the first time. Carnegie Mellon University (CMU) computer scientists are now working to redesign CAPTCHAs to create a more secure system. The first redesign, known as reCAPTCHA, uses the Google Books Project and the Internet Archive to find words that the two projects' OCR systems were unable to recognize. Human users are asked to identify these words to sign up for Web sites, helping complete the two projects' digitalization of older books in the process. CMU researchers also are exploring image-based CAPTCHAs. The ESP-PIX system requires users to pick a word that describes four objects in an image, and the SQ-PIX system asks users to choose one image from a group of three and trace the outline of the object within the image. However, the researchers say these systems still have some flaws, since people can easily create abnormal descriptions or lack the dexterity to accurately trace an image onscreen.

Advocates Worry Electronic Voting Allows Fraud
Medill Reports (01/21/09), J. Barker

Many election officials in the United States would like to see a return to paper-ballot voting, which they say is faster and more reliable that touch-screen voting. Illinois state representtative M. Boland wants to limit touch-screen machine use to handicapped voters, and is calling for stricter recount policies after witnessing problems in Ohio and other states. Current Illinois law requires an automatic recount of 5% of an election's vote. Boland and the Illinois Ballot Integrity Project (IBIP) want to raise the recount to 10% of the vote. Illinois precincts offer voters two options at the polls. Touch-screen machines provide voters with an ATM-like interface that voters press to make their choices and receive a grocery-style receipt. Voters can either confirm the receipt or vote again. Voters also have the option of voting on a traditional paper ballot that is read by an optical scanner. In DuPage county, most voters chose the optical scanner. IBIP's Robert Wilson says the organization opposes touch-screen voting because of its cost, inaccuracy, and security concerns. The IBIP is primarily concerned because there is no review of the software used in touch screen voting, says IBIP's M. Urda. Urda says the machine's software "is so porous that someone with a cell phone could hack into it."

A Tool to Verify Digital Records, Even as Technology Shifts
New York Times (01/27/09) P. D3; J. Markoff

University of Washington researchers have released the first component of a public system that will provide authentication for an archive of video interviews with prosecutors and other members of the International Criminal Tribunal on the Rwandan genocide, along with the first portion of the Rwandan archive. The system will be available for others to digitally preserve and authenticate first-hand accounts of war crimes, atrocities, and genocide. The tools are needed because advancements in technology have made it possible to alter digital text, video, and audio in nearly undetectable ways. The researchers say the system means the authenticity of digital documents such as videos, transcripts of personal accounts, and court records can be indisputably proved for the first time. The researchers have created a publicly available digital fingerprint, known as a cryptographic hash mark, that will make it possible for anyone to determine that the documents are authentic and have not been tampered with. The digital hash concept was first conceived by IBM's H.P. Luhn in the early 1950s, and the researchers are the first to attempt to simplify the application for nontechnical users and offer a complete system for long-term data preservation. Similar efforts to preserve a complete record of the World Wide Web and other documents led to computer scientist B. Kahle launching the Internet Archive in 1996. Another digital preservation effort was launched by Stanford University librarians in 2000. Their system, dubbed LOCKSS, for Lots of Copies Keep Stuff Safe, preserves journals by distributing copies of documents over the Internet to an international community of libraries.

ICANN Ponders Ways to Stop Scammy Web Sites
IDG News Service (01/27/09), J. Kirk

ICANN recently issued an initial report on fast flux, a technique that is being exploited by hackers and other cybercriminals. Fast flux allows a Web site's domain name to resolve multiple Internet Protocol (IP) addresses. Content distribution networks use the technique legitimately in order to balance loads, lower data transmission costs, and improve performance. However, cybercriminals are using the technique to make it more difficult for Internet service providers to shut down illegal Web sites. Fast flux helps cybercriminals avoid detection and frustrate efforts to close their Web sites. Internet security experts are trying to develop a way to stop the criminal use of fast flux without restricting the technique's legitimate uses. Potential solutions include quicker identification of abusive domain names or limiting the ability of registrants to repeatedly change name servers.