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

Δελτίο 118
30 Μάη 2008

Alarming Open-Source Security Holes
Technology Review (05/20/08), S. Garfinkel

An open-source programming error made in May 2006 that reduced the amount of randomness used to create cryptographic keys in the widely used OpenSSL library have created serious security vulnerabilities in at least four open-source operating systems, 25 applications programs, and millions of computer systems. Although the vulnerability was discovered on May 13 and a patch has been distributed, installing the patch does not repair damage to the compromised systems and some computers may be compromised even though they are not running the code. Modern computer systems use large numbers to generate keys that are used to encrypt and decrypt data sent over a network. The error reduces the number of different keys that Linux computers can generate to 32,767, making it significantly easier for hackers to guess the key. Moreover, keys created by the computers with the error are not fixed when the patch is installed. It's impossible to know how many computers are affected because vulnerable keys could have been transferred to non-open source systems if a file encrypted by the flawed system was transferred to another system. The error was made when programmers incorrectly used a tool that was intended to catch programming bugs that lead to security vulnerabilities. Programs that use OpenSSL include the Apache Web server, the SSH remote access program, the IPsec Virtual Private Network, secure email programs, and many others.

Proponents, Critics Give No Ground in Tussle Over E-voting
Computerworld (05/19/08) Vol. 42, No. 21, P. 12; T. Weiss; G. Gross; R. McMillan

Advocates and critics of touch-screen voting systems are refusing to budge on their opposing views about the technology's reliability, with the former continuing to testify to its accuracy and security while the latter maintain their position that susceptibility to hacking and miscounts are among the risks users of e-voting systems run. Two studies released in March from The Brookings Institution and InfoSentry Services conclude that most voters are comfortable with touch-screen systems, while G. Bartlett with the North Carolina State Board of Elections says "the routine voter has not expressed any dissatisfaction with or distrust of any type of e-voting equipment." Skeptics counter that such studies are irrelevant because they are based on people's beliefs and feelings rather than on hard facts. Experts such as Johns Hopkins University professor A. Rubin say the chief problem with e-voting systems is the absence of any way for voters to assuredly know that their votes are being counted properly. Election Technology Council executive director D. Beirne contends that many e-voting opponents "are only focusing on the perceptions" of problems. In some cases election officials are the ones doubting the technology's reliability, while e-voting vendors and other supporters are quick to say that human rather than technical error is usually the cause of problems with e-voting machines.

Homeland Security Helps Reduce Open Source Flaws
InternetNews.com (05/20/08), S.M. Kerner

A Dept. of Homeland Security multi-year initiative intended to improve open source code quality, launched over two years ago, has reduced the defect density in 250 open source projects by 16%, essentially eliminating over 8,500 defects, Coverity reports. The report comes at a time when open source software is becoming an increasingly integral part of critical infrastructure in government and private enterprise. Coverity runs scanning tools on the open source projects included in the initiative to find coding errors. While many of the projects have benefited from running Coverity's scans, not every project has managed to reduce errors, primarily because they have not been actively using the results from the scan. Projects working in Perl, PHP, Python, Postfix, Samba, and TCL have been able to reduce their code defect densities by using data from the Coverity scans. Coverity found a clear pattern indicating that certain errors occur more often, specifically Null Point Dereferences, which occurred 28% of the time. The Coverity report says this error often occurs when one code path initializes a pointer before its use, but another code path bypasses the initialization process. The second most common defect is resource leaks, at 26% of all defects, which often involve failure to release resources when the initial allocation succeeds.

Researchers Find New Ways to Steal Data
IDG News Service (05/19/08), R. McMillan

Researchers at the University of California, Santa Barbara (UCSB) and Saarland University in Saarbrucken, Germany, have found unconventional ways of stealing data. In Saarbrucken, the researchers have been able to read computer screens using reflections on objects such as glasses and teapots. Meanwhile, UCSB researchers have created Clear Shot, software that analyzes a video of hands typing on a keyboard to determine what was being written. Clear Shot was inspired by the movie "Sneakers," in which R. Redford's character obtains a video of his potential victim typing in his password and says he is going to get a "clear shot." Clear Shot can analyze video of hand movements on a computer keyboard and transcribe them into text. UCSB graduate student Marco Cova says Clear Shot is accurate about 40% of the time. The software also suggests alternative words that may have been typed. Saarland University professor M. Backes says his research began as a fun project to see if he could tell what other people were working on by watching windows near computer monitors. The researchers soon found that using a $500 telescope focused on a reflective object in front of a monitor could create readable images of Word documents. The researchers are now working on new image analysis algorithms and using astronomical cameras in the hopes of getting better images from more difficult surfaces such as the human eye.

Inside Lockheed Martin's Wireless Security Lab
Network World (05/19/08), B. Reed

Lockheed Martin's Wireless Cyber Security Lab is engaged in a race with hackers to catch flaws and vulnerabilities in wireless security in the hopes of correcting them before they are exploited. "We're trying to ensure that something similar [to 9/11] doesn't happen in the realm of wireless communications," says lab director J. Morrison. Lockheed Martin's P. Nijeb says the biggest nascent wireless security threat is the blurring of the boundary between home and the office, as employees increasingly access company data via corporate VPNs from their residences. To address this problem, the company has been testing numerous types of consumer technology, including cell phones, which have been moving to enterprise networks, and the spread of Wi-Fi hot spots has been of particular concern because of the technology's growing ubiquity in urban areas. Nijeb cites "connection hijacking, deliberate or inadvertent denial of service, the creation of security holes in corporate or government net-

works, and difficulty in attributing network actions to specific IP addresses, due to the ease of hijacking" as major issues with Wi-Fi, which Morrison says can add up to immense burdens for corporate IT departments that fail to educate their users about security matters. Lockheed Martin R&D investigator J. Crawford says the proliferation of Bluetooth technology is also a worrying trend, as products capable of picking up Bluetooth signals outside their transmission range could theoretically be used to track people. The problems that Lockheed Martin's wireless security lab is focusing on are also challenges for the US military, particularly as they relate to the security of its battlefield communications networks. Morrison says soldiers' vulnerability is highest when they use wireless communications in crowded urban settings, which parallels the risk corporate users run when they link to enterprise networks using home-based Wi-Fi connections.

Cryptography Expert Wins ACM Award for Advances in Protecting Privacy of Information Retrieval, AScribe Newswire (05/22/08)

ACM has named Microsoft Research Silicon Valley Lab researcher S. Yekhanin the winner of the 2007 Doctoral Dissertation Award. Yekhanin has developed a new way to keep a query private when the user is accessing a public database. With new families of private information retrieval schemes and a special kind of error-correcting codes known as locally decodable codes, the research supports the kind of anonymity that will improve the security and use of cyber-infrastructure. The research has also helped further protection for data storage, secure multi-party computation, and computational complexity. MIT nominated Yekhanin, whose dissertation is titled "Locally Decodable Codes and Private Information Retrieval Schemes." He will receive the Doctoral Dissertation Award and its $20,000 prize at the annual ACM Awards Banquet on June 21, 2008, in San Francisco, California. B. Applebaum, a post doctoral candidate at Princeton University, Y. Liu, a research staff member at IBM Research, and V. Conitzer, assistant professor of computer science and economics at Duke University, received honorable mention and will each receive a $10,000 prize.

E-Voting Banned by Dutch Government
InterGovWorld.com (05/21/08), A. Udo de Haes

The Netherlands has banned the use of electronic voting machines in future elections due to concerns that the technology was too vulnerable to eavesdropping. "Developing new equipment furthermore requires a large investment, both financially and in terms of organization," according to the Ministry of Internal Affairs. "The administration judges that this offers insufficient added value over voting by paper and pencil." The Dutch government also banned voting printers, which were criticized by a group of experts led by B. Jacobs, a professor at Radboud University in Nijmegen, over similar security concerns. The Netherlands will make use of electronic vote counting, and will conduct tests to improve its effectiveness. The local activist group "Wij vertrouwen stemcomputers niet" (We don't trust voting computers), led by computer hacker R. Gonggrijp, declared the decision a victory for those who want verifiable election results.

Experts Warn of Cyber Terrorism Threat
Associated Press (05/20/08), J. Zappei; C. Vatvani

The International Multilateral Partnership Against Cyber Terrorism, which involves both public and private groups from the around the world, will create a new center in Malaysia to fight cyber-terrorism. The center is likely to open by the end of 2008 and will provide such

services as emergency response and training. Information technology has changed how terrorists operate, said H. Toure, secretary general of the United Nations' International Telecommunication Union, at a May 20 conference in Malaysia attended by representatives from more than 30 countries. He said that cybersecurity needs to be incorporated into "every aspect of keeping ourselves, our countries, and our world safe." Malaysian Prime Minister A. A. Badawi said that nations must work together to safeguard facilities such as nuclear power plants, dams, telecommunication networks, and energy services from cyber-terrorism.

Army Aims to Take Guesswork Out of Cyber-defense
Government Computer News (05/20/08), W. Jackson

The Cyber-Threat Analytics (Cyber-TA) project, funded by the Army Research office, will create a global system to gather and correlate security events to provide users with early warnings on upcoming attacks, as well as aid in the configuration on sensors, filters, and other devices intended to detect and respond to such events. The project's goal is to create software that can be used to help program security devices. L. Ricciulli, chief scientist at MetaFlows, a project participant, compares the Cyber-TA's tools to Google's page-ranking algorithms, and says the project is applying similar principles to cybersecurity warfare. Open-source organization Emerging Threats is also participating in the project, providing specialized threat signatures to complement signature updates from Sourcefire for its open-source Snort intrusion detection and prevention system. Ricciulli says the project wants to create a way of configuring sensors with a global understanding of what is happening around them. MetaFlows is updating previous Cyber-TA research by expanding algorithms for programming network security devices. The project is funded through the end of 2009, and additional National Science Foundation funding will last through 2010.

Senators: No Need for Paper E-Voting Trails, 'Electronic' Ones Are OK
CNet (05/23/08), A. Broache

Senators D. Feinstein (D-Calif.) and B. Bennett (R-Utah), who lead a Senate committee that oversees election law, say they will introduce a bill that requires precincts using touch-screen or direct-recording electronic voting machines to equip them with independent paper, electronic, audio, video, or pictorial records that would allow voters to verify their selections. ACM advisory committee member and Princeton University professor E. Felten said that he could not comment on the new bill without seeing more details first. The bill indicates that the senators at least partially acknowledge the argument that paper trails are not the only option for independently verifying a voter's selections and that other innovative technologies could emerge in the future. The bill may also be intended to appease state and local election officials who frequently complain about the costs associated with outfitting their machines with paper trails. In addition to a verification system, the bill would require states to provide public audits of their election results, would establish certain security requirements for the voting machines and their software, and would establish a research grant program designed to encourage the development and testing of new technologies for verifying votes. The bill would take effect on January 1, 2012, but states could request a waver that would extend the deadline to the beginning of 2014.