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

Δελτίο 98
30 Νοέμβρη 2007

Adding Math to List of Security Threats
New York Times (11/17/07) P. B4; J. Markoff

Weizmann Institute of Science professor A. Shamir recently warned of a hypothetical incident in which a math error in a commonly used computing chip could endanger the security of the global electronic commerce system. Shamir, one of the designers of the RSA public key algorithm, says the increasing complexity of microprocessor chips will almost certainly lead to undetected errors. Similar errors have already been found in older systems, such as the discovery of an obscure division bug in Intel's Pentium microprocessor in 1994 and a multiplication bug found in Microsoft's Excel spreadsheet. A subtle math error would allow an attacker to break the public key cryptography technique by discovering the error in a widely used chip and sending a "poisoned" encrypted message to the computer, allowing the attacker to compute the value of the secret key used by the targeting system. Shamir says the error would allow millions of PCs to be attacked without having to manipulate the operating environment of each one individually. Shamir notes that laws governing trade secrets that protect the exact workings of microprocessor chips make it almost impossible to verify that the chips have been designed correctly. "Even if we assume that Intel had learned its lesson and meticulously verified the correctness of its multipliers," he says, "there are many smaller manufacturers of microprocessors who may be less careful with their design."

Synchronized Shaking Connects Gadgets Securely
New Scientist (11/13/07), T. Simonite

Lancaster University researchers have developed software that allows two cell phones to establish a wireless connection by holding the devices together and vigorously shaking them. The shaking movement is measured by built-in accelerometers. By holding the two devices together tightly the accelerometer readings will match, enabling the system to make a secure connection either by transmitting an open stream of accelerometer data and searching for matching data, or by establishing a secure connection automatically and then using accelerometer measurements to confirm it. The researchers say this technique is both easier and more secure than selecting a device from a list or entering a security code, and could make it easier to connect cell phone peripherals such as wireless headsets. Currently, users have to select the device from a list and enter a PIN supplied with the device. However, about 95% of headsets have "0000" as their default PIN code, creating a security weakness. Lancaster University's R. Mayrhofer says some cell phones already include accelerometers and adding the software needed for shake-to-connect should be relatively simple. Eventually, shake-to-connect could be used for more sensitive transactions such as transferring money between credit cards.

Google Meets Sherlock Holmes
Newswise (11/13/07)

Most of the information that hinted at possible trouble prior to the 9-11 attacks was buried under massive amounts of data being collected faster than analysts could handle. A single day's collection would fill more than 6 million 160-gigabyte iPods, and some of the data conflicted with other pieces of information. To prevent such pieces of information from being missed again, researchers at the DHS Science and Technology Directorate are developing ways of viewing such data as a 3D picture where important clues are more easily identified. Mathematicians, logicians, and linguists are collaborating to make the massive amounts of data form a meaningful shape, assigning brightness, color, texture, and size to billions of known and apparent facts. For example, a day's worth of video, cell phone calls, photos, bank records, chat rooms, and emails may be displayed as a blue-gray cloud with links to corresponding cities. "Were not looking for 'meaning' per se," says Dr. J. Kielman, Basic Research Lead for the Directorate's Command, Control and Interoperability Division, "but for patterns that will let us detect the expected and discover the unexpected." Kielman says it will still be several years before visual analytics can automatically create connections from fuzzy data such as video.

Tracing Terrorists' Social Web
Associated Press (11/18/07), A. Rotstein

There are currently tens of thousands of Web sites devoted to delivering the beliefs and methods used by terrorist organizations, and tracking and monitoring these Web sites and chat rooms is a extremely difficult task for government agencies. While the sites may not appear to reveal any information on their creators, programmers and writers leave digital clues such as the words they chose, punctuation, syntax, and how they code multimedia attachments and Web links that can be used to find them. University of Arizona researchers are working on a tool that would use these clues to automate the analysis of online jihadism. The Dark Web project aims to search sites, forums, and chat rooms to find the Internet's most influential jihadists and learn how they attract new recruits. Artificial Intelligence lab director H. Chen hopes Dark Web will cripple the online terrorist recruitment and education effort, as many potential terrorists learn how to make explosives and plan attacks online. "Our tool will help [US authorities] ID the high-risk, radical opinion leaders in cyberspace," Chen says. Former FBI counterterror chief D. Watson says the ability to sort through massive amounts of data automatically would be of great value, as terrorist Web sites and communications are currently analyzed manually. "It would greatly enhance the speed and capability to sort through a large amount of data," Watson says. "The issue will be where is the Web site originating and where are the tentacles going?"

12 Spam Research Projects That Might Make a Difference
Network World (11/20/07), C. Garretson

Numerous antispam projects are being conducted to help make email a safer and more enjoyable process, with some projects aiming to close existing weaknesses such as image spam and phishing, while others work to prevent future vulnerabilities. The University of Pennsylvania has released a research paper that describes how filters can be adjusted to determine if an inbound message contains image spam, including the use of an algorithm that can select features for classification based on speed and predictive power. Princeton University researchers have proposed a detection system that relies on traditional antispam filtering, but duplicates the randomization algorithms image spam exploits to look like similar images. Georgia Tech is using a discriminative classifier learning approach to image modeling to identify image spam by analyzing images extracted from a body of spam messages and identifying key image properties. The University of Cagliari in Italy is using low-level image processing techniques to recognize content-hiding tricks such as character breaking and character interference. To fight phishing, Carnegie Mellon University has been examining why phishing attacks work and has developed an online game designed to teach Internet users about the dangers and techniques used in phishing attacks. Dartmouth has suggested using an anonymous credentialing system that can blacklist misbehaving users without requiring the involvement of a TTP, and Georgia Tech has proposed having blacklisting techniques adapt to changes in spam by using a filtering system called SpamTracker, which tracks email uses based on their sending behavior rather than their identity. IBM research is investigating combining global and personal antispam filtering systems. Another project by Carnegie Mellon, with assistance from the University of California at San Diego, is studying the underground economy that nourishes credit card fraud, identity theft, spamming, phishing, online credential theft, and the sale of compromised hosts.

Internet Users Give Up Privacy in Exchange for Trust
Economic & Social Research Council (11/26/07)

New research funded by the Economic and Social Research Council suggests that Internet users are likely to provide more personal information online if they consider the Web site to be trustworthy. "Even people who have previously demonstrated a high level of caution regarding online privacy will accept losses to their privacy if they trust the recipient of their personal information," says Dr. A. Johnson, head of the Privacy and Self-Disclosure Online project. However, Internet users who have some concerns about a Web site will become more guarded alter their behavior. The way in which questions are worded and response options are designed, such as giving Internet users the opportunity to choose "I prefer not to say" or select their salary from a broad scale, often results in users providing as little information about themselves as possible. "One of the most interesting aspects of our findings is that even people who genuinely have a high level of concern regarding privacy online may act in a way that is contrary to their stated attitudes when they come across a particular set of conditions," Joinson says. The level of trustworthiness may ultimately determine the degree of helpful information that online services obtain from people who visit their Web sites.

Standards Suggested for Writing Secure Java
Network World (11/20/07), T. Greene

The Secure Programming Council has created a series of documents that outline the skills coders need to write Web applications that are more capable of withstanding attacks. The first of these documents was released earlier this month and lists the skills that the council believes are essential to writing Java and JavaEE code that is free of flaws that hackers could exploit. SANS Institute director of research A. Paller says that some schools and groups offer secure coding courses, but the curriculums are developed based on the instructors' knowledge and best efforts, often contain security gaps, and do not adhere to industry standards for what the course should include. Paller says the Secure Programming Council documents are intended to address such shortcomings by drawing from existing texts as well as input from secure-coding trainers and businesses that work to train in-house programmers in secure training. "It's a common body of what people need to know, benchmarks for employers and teachers," Paller says. The Java paper, "Essential Skills for Secure Programmers Using Java/JavaEE," focuses on data dandling, authentication and session management, access control, Java types and virtual machine management, application faults and logging, encryption services, and secure architecture and coding principles. Future papers will cover C, C++, .Net languages, Perl, and PHP.

Researcher Lands Computer Security Grant From Air Force
University of Texas at Dallas (11/18/07)

The US Air Force has awarded a $350,000 grant that will enable University of Texas at Dallas computer science professor K. Hamlin apply his computer security technology to larger applications and more computer architectures. Over the next three years, Hamlen will use the grant money to transition older programming languages to today's safer languages. "It's extremely difficult to write a program that does not have vulnerabilities in it, mainly because these languages were designed in the 70s and early 80s when nobody was thinking about computer security," Hamlen says. His technology is designed to automatically rewrite untrusted code before execution, which preserves the functionality of the program and effectively disables any malicious code. He has spent the last several years working on the rewriting technology. The grant money comes from the Air Force's Young Investigator Research Program, which targets talented scientists and engineers who have received PhDs within the last five years.