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

Δελτίο 124
31 Ιουλίου 2008

When the Phone Goes With You, Everyone Else Can Tag Along
Washington Post (07/12/08) P. A1; E. Nakashima

The launch of the iPhone 3G highlights the growing sophistication of the cell phone and mobile device industry, but also presents new privacy concerns. The iPhone combines GPS functions with the Internet to create a feature that not only pinpoints a location but displays nearby attractions. These features and the information they generate could be used by merchants to target ads, malls to attract shoppers, insurance adjusters to calibrate premiums, or parents to keep track of children. However, many consumers may not realize that by sharing this information they are creating permanent records that network providers, social Web sites, law enforcement, and others could potentially use to track everywhere they have been. "There's a disconnect between our expectations of when we will be observed and who will be observing us and how that information will be used and what the technology is allowing companies to do," says University of Southern California law professor Jennifer Urban. Connected devices such as the iPhone could allow users to locate nearby friends, find nearby events, or access "geo-tagged" photos taken and uploaded by others at the same location. As this information migrates from cell phones to social networking sites, the information suddenly becomes available to hundreds of people, instead of the small number of people who know the user and have his or her cell number. However, the technology continues to inspire researchers. At Microsoft, researchers have collected four years' worth of GPS data from volunteers to build models that estimate road speeds on Seattle-area streets and highways to better understand traffic flow. The wireless industry has guidelines for location-based services that stress consumer notification, consent, and data security, but self regulation is only part of the solution. Security experts say baseline federal legislation is needed to cover all firms that collect personal electronic data.

Printer Dots Concern Privacy Advocates
USA Today (07/14/08) P. 3A; T. Frank

An increasing number of manufacturers are building color laser printers with technology that leaves microscopic yellow dots on each printed page to identify the printer's serial number as well as the date and time the page was printed, says the Electronic Frontier Foundation. The technology has existed for years, but the declining price of color laser printers is making the practice a greater consumer threat. The dots can be seen using a blue LED light to allow the Secret Service to investigate counterfeit bills made with laser printers. Privacy advocates say the technology could be abused and used to identify political dissidents, whistleblowers, or anyone else who prints materials that authorities want to track. Electronic Frontier Foundation computer programmer S. Schoen says there is nothing about the technology that limits its application to counterfeit investigations, and warns that people who are not doing anything wrong could have their privacy threatened. Schoen's tests show that the dots are produced by 111 color laser printers made by 13 companies. Xerox's B. McKee says the dots are often a requirement to do business internationally, while the Secret Service's L. Pagano says the agency is the only US body with the ability to decode the information printed in the dots.

Goodbye to Faulty Software?
ICT Results (07/15/08)

A team of European researchers believes that it will be possible to create software that is guaranteed to be free from bugs. "The software industry is still very immature compared to other branches of engineering," says Chalmers University computer scientist B. Nordstrom. Nordstrom believes the entire approach to software design needs to be rethought, replacing the usual approach of validating a program through a lengthy testing process with a design philosophy that guarantees from first principles that a program will act as it should. The key is a reformation of mathematics called type theory based on the notion of computation, in which the specification for a computational task is stated as a mathematical theorem. The program that performs the computation is essentially the proof of the theorem, and by proving the theorem the program is guaranteed to be correct. The European Union has funded a series of projects to develop type theory since 1989. Nordstrom was coordinator of the TYPES project, which supported cooperation on type theory between researchers at 15 European universities and research institutes and 19 associated academic and industrial organizations. TYPES has released several open source programs, including proof editors that, in type theory, are the key to guaranteeing bug-free programs. "This is a very slow process, it takes many years to get ideas from the universities into industry, but I think it's slowly taking place," Nordstrom says.

Enigma Variations
Economist (07/10/08) Vol. 388, No. 8588, P. 88

The development of a photon detector by A. Shields and colleagues at Toshiba's research laboratory in Cambridge, England, is viewed as an important step in the enablement of practical quantum cryptography, which promises unbreakable codes for messages. The device can count single photons at room temperature, and represents a simple tweaking of the design for avalanche photodiodes that are being used to detect multiple photons, which should ease implementation. In an avalanche photodiode, the striking of a semiconductor by photons can be read by detecting positively charged "holes" in the crystal lattice left by the displacement of electrons caused by the photonic impact, but determining the number of photons that have arrived requires analysis of the signal just after it has been formed. Shields has tackled this challenge through a technique that filters out noise and allows the signal to be extracted. Without a practical photon counter, photon repeaters that do not destroy quantum states cannot be constructed. Shields' device allows cryptographers to harness the phenomenon of quantum entanglement, in which photons share quantum states, to support this breakthrough.

DNS Flaw Discoverer Says More Permanent Fixes Will Be Needed
Computerworld (07/17/08), J. Vijayan

D. Kaminsky, a security researcher at IOActive who recently discovered a previously unknown cache-poisoning vulnerability in the Internet's Domain Name System (DNS) protocol, warned IT managers at a press conference on July 17 that while patches have been released to address the flaw, more may need to be done to address the issue over the next several months. Kaminsky noted that the patches that were issued in the wake of the discovery of the flaw earlier this month are at best a temporary measure aimed at protecting the DNS infrastructure from hackers trying to exploit the flaw, which exists in a transaction identification process that the DNS protocol uses to determine whether responses to DNS queries are legitimate. Kaminsky said that while DNS messages include what are supposed to be random identification numbers, only about 65,000 different values are currently being used as identifiers. Compounding the problem is the fact that the process of assigning identifiers to packets is not especially random and can be guessed, Kaminsky said. If hackers are able to identify the identification numbers on DNS messages, they could introduce forged data into the DNS system and redirect Web traffic and email to systems they control. Although the patches that aim to correct this vulnerability appear to be working, there are people who have gotten very close to exploiting it, Kaminsky said. As a result, IT managers should expect to see more security patches that aim to correct the flaw over the next several months.

Google Is Watching, Perhaps Soon in Your Home
InformationWeek (07/11/08), T. Claburn

A recent paper, co-authored by Google researcher B. Schilit and computer scientists J. Yang from the Georgia Institute of Technology and D. McDonald from the University of Washington, proposes "home activity recognition," a system that would track people's activities at home through home network interactions. "Activity recognition is a key feature of many ubiquitous computing applications ranging from office worker tracking to home health care," the paper says. "In general, activity recognition systems unobtrusively observe the behavior of people and characteristics of their environments, and, when necessary, take actions in response - ideally with little explicit user direction." Home monitoring could be used to remind people to perform forgotten tasks, help them remember information, or encourage them to act more safely. However, the concept raises several privacy questions, including how the data will be protected, who will have access to the data, and what will prevent the data from being subpoenaed or stolen. The paper provides a sample of the type of data that could be collected, similar to a Web history log that records the use of devices attached to a home network. "Going forward we are eager to find alternative sources for interaction event capture," the paper says. "Rather than just waiting for the desktop operating systems to accommodate user activity tracking, we see the Web platform as a potential shortcut to a friendlier environment for activity capture."

Software Helps Developers Get Started With PIV Cards
National Institute of Standards and Technology (07/09/08), E. Brown

Two software programs have been developed by the National Institute of Standards and Technology (NIST) that demonstrate how Personal Identity Verification (PIV) cards can be used with Windows and Linux systems to perform logon, digital signing, verification, and other services. The software is intended to assist software developers, system integrators, and computer security professionals in the development of products and solutions in response to Homeland Security Presidential Directive 12 and the FIPS 201-1 standard. NIST collaborated with the industry to develop the standards for the PIV cards that will be used for the directive. Each card contains a unique number, two of the employee's biometric fingerprint templates, and cryptographic keys stored on an embedded chip. NIST's D. Dodson says the agency wanted to provide IT professionals with a model of how PIV cards can be used to support authentication to federal information systems. Each federal agency will implement the use of PIV cards on its own schedule. NIST developed the demonstration software to show that PIV cards can work with common computer activities. For example, user name and password can be replaced with the user inserting his or her PIV card in a reader and entering a personal identification number, which could eliminate the need for passwords for other applications and provide access to secure databases for authorized users.

ReCaptcha: Reusing Your 'Wasted' Time Online
CNet (07/16/08), S. Olsen

The goal of the ReCaptcha project is to use captcha technology--distorted word puzzles that humans can successfully solve but machines such as spam bots cannot--to improve machines' identification of scanned text that a computer has trouble recognizing optically due to faded ink or blurriness, so that print archives can be more effectively mined by search engines. Carnegie Mellon University (CMU) professor and ReCaptcha creator L. von Ahn says up to 600 million people have completed at least one ReCaptcha on sites that use the technology in the last year, and such activity is aiding and expediting ambitious text-scanning initiatives such as the New York Times digitization project. Von Ahn debuted the ReCaptcha free antispam system with a double-word test in 2007, and this test allows the system to formulate a confidence rating for the human by presenting one word the computer does not know with another it does know. People type 200 million captchas globally every day by von Ahn's calculations, while the incredible amount of time people spend playing games drove the CMU professor to initiate a project to tap this pastime to tackle major computational challenges. One game borne from that project, the ESP Game, was designed to enhance Web search using image labeling by asking two randomly paired people on different systems to describe the same image without any communication, and to predict the same word for the image within a time limit. Von Ahn and a group of CMU computer scientists have rolled out four new games to address different challenges in the field of artificial intelligence partly due to the success of the ESP Game.

Details of Major Internet Flaw Posted by Accident
IDG News Service (07/21/08), R. McMillan

On July 21, a computer security company accidentally published details of a major flaw in the Internet's Domain Name System (DNS), several weeks before the error was supposed to be disclosed. The flaw was discovered several months ago by IOActive researcher D. Kaminsky, who has been working with Internet software vendors, including Microsoft and Cisco, and the Internet Systems Consortium to fix the problem. The companies released a patch for the bug a few weeks ago, and encouraged corporate users and Internet service providers to patch their DNS systems as soon as possible. When announcing the discovery of the flaw, Kaminsky asked members of the security research community to withhold public speculation on the precise nature of the flaw to give users time to patch their systems, and he planned on disclosing details of the flaw during a presentation at the Black Hat security conference on Aug. 6. Some researchers took Kaminsky's request as a personal challenge to find the flaw before Kaminsky revealed it, while others complained about being kept in the dark about the technical details. On July 21, Zynamics.com CEO T. Dullien made a guess about the bug, admitting that he knew very little about DNS, but his findings were quickly confirmed by Matasano Security, a vendor that had been briefed on the issue. Matasano made a post that acknowledged Dullien's identification of the flaw, but the post also contained technical details of the bug, saying that an attacker could use a fast Internet connection to launch what is known as a DNS cache poisoning attack against a Domain Name server and succeed, for example, in redirecting traffic to malicious Web sites within about 10 seconds. The attack takes advantage of several known DNS bugs and combines them in a novel way.

CCTV Camera Identifies People by Race
IDG News Service (07/14/08), J. Kirk

London's Royal College of Art engineer B. Males has written software for the RTS-2 (Racial Targeting System), a camera that determines a person's race. Males says he built the system in an attempt to raise awareness of privacy issues among the public, which often is unaware how frequently it is surveyed by closed-circuit TV (CCTV), particularly in the United Kingdom. Males bought a CCTV camera from eBay and wrote the software for the program using C++, partially using Intel's Open Source Computer Vision Library. Males put the camera on a motor so it can follow people as they walk past the camera, which supplies an image of a person's face to a laptop. Software then takes a color sample from the subject's nose and cheeks and averages the pixel values to determine the person's race. Males has taken the portable system to places such as Covent Garden and Kensington High Street in London, areas that are popular with tourists and shoppers. Nearly everyone who passed by either did not notice the camera or barely paid attention, evidence that shows how people are used to being monitored, Males says. "The device isn't that sophisticated," he says. "This software exists at a much more sophisticated and dangerous level in the commercial world."

Attack Code Released for New DNS Attack
New York Times (07/24/08), R. McMillan

Developers of the Metasploit hacking toolkit have released an attack code that exploits a recently disclosed flaw in the Domain Name System. Internet security experts warn that this code could be used to launch virtually undetectable phishing attacks against Internet users whose service providers have not installed the latest DNS server patches. The bug could be used to redirect users to fake software update services to install malicious software on their computers through a technique called cache poisoning. The bug was first disclosed by IOActive researcher D. Kaminsky in early July, but technical details of the flaw were recently leaked, allowing for hackers to create the attack code. Kaminsky had worked with major DNS software providers like Microsoft, Cisco, and the Internet Systems Consortium for several months to create a patch for the problem before the flaw was known to the public. Corporate users and Internet service providers who are major users of DNS servers have had since July 8 to patch the flaw, but many have not finished installing the patch on all DNS servers. ISC president P. Vixie says that most people have not patched yet and that this flaw is a "gigantic problem for the world."

Data Can Leak from Partially Encrypted Disks
IDG News Service (07/16/08), R. McMillan

Encrypted data can spill over into unencrypted parts of a computer, exposing it to hackers and viruses, according to researchers from the University of Washington and British Telecommunication. Essentially, a computer is not fully protected unless it is 100% encrypted, says study co-author T. Kohno. "I suspect that this is a potentially huge issue. We've basically cracked the surface," says Kohno, an assistant professor at the University of Washington's Seattle campus. When a user opens an encrypted file with Word, Google Desktop, or even an encrypted USB drive, the information can still be stored in unencrypted areas of the hard drive. During their experiments, researchers viewed encrypted Word documents by opening the auto-recovery folder and read encrypted files over Google Desktop when the Enhanced Search option was on. Even encryption software platforms like TrueCrypt 5.1a contain the same vulnerabilities, researchers found, and the software version 6.0 addresses some problems but still does not fully protect encrypted data on an unencrypted computer.

Dartmouth Begins Network Security Project

Access Control & Security Systems (07/15/08)

A new research project at Dartmouth College promises to reveal key information on how the campus wireless computer network is used and how to provide better security. The Dartmouth Internet Security Testbed (DIST) will give campus researchers an opportunity to monitor live network activity at scale and in real time, says D. Kotz, professor of computer science and the principal investigator on the DIST initiative. "We've worked in laboratory settings with controlled parameters; now it's time for a live, real-world test," adds Kotz. The team will develop and test sensing technology for gathering real-time data, and could learn how to quickly discover malicious activity and the best way to respond to such situations. The project will provide a model for how other enterprises can secure their wireless networks, and will help improve network security technology and practices for using the Internet. The Dept. of Homeland Security is funding DIST through Dartmouth's Institute for Security Technology Studies. "We've ensured that strict processes are in place to monitor the project to protect the privacy of our Wi-Fi users," says Kotz.

Researcher to Demonstrate Attack Code for Intel Chips
IDG News Service (07/14/08), S. Lemon

A security researcher at this year's Hack In The Box (HITB) Security Conference in Kuala Lumpur, Malaysia, will demonstrate how to attack a computer through vulnerabilities in Intel's microprocessors. K. Kaspersky plans to show attendees of the October conference how processor bugs, or errata, can be manipulated to give an attacker full access on the kernel level or even take down a system. The risk from these kinds of attacks is rising, and processors may carry hundreds of millions of errata without ever being aware of their existence. "It's possible to fix most of the bugs, and Intel provides workarounds to the major BIOS vendors," Kaspersky states. "However, not every vendor uses it and some bugs have no workarounds." Kaspersky's proof-of-concept attack will take place on a spectrum of operating systems that use JavaScript or TCP/IP packets. These systems include Windows XP, Vista, Windows Server 2003, Windows Server 2008, Linux, and BSD.

Keeping Up With Your Peers, Securely
ICT Results (07/21/08)

European researchers have built a platform that can be used to develop secure, mobile peer-to-peer (P2P) applications for specific industry needs. With secure P2P, users will not have to go through a central communications hub to connect and work together. The European Union-funded PEPERS project developed the platform on mobile devices based on the open-source Symbian operating system for mobile use. "And developing software that responded to all the security constraints was tough, too," says PEPERS project coordinator V. Tountopoulos. "We had the rules in place, but then you need to adapt those rules to a specific situation." The PEPERS researchers addressed the issue by isolating the P2P application from the rest of the host operating system, which improved security, and they also faced certain business constraints. The team used the platform to develop a P2P application that would allow reporters to collaborate on breaking news and another that would allow security guards to coordinate a response to a situation without the use of a central dispatch.

RFID Unlocks Supply Chain Potential
ICT Results (07/17/08)

The European Union-funded SMART project is completing a radio-frequency identification (RFID) application platform that addresses a number of technical problems associated with RFID, and presents options for an integrated solution for businesses. RFID could revolutionize store management through stock management, sophisticated promotions, and supply chain optimization, but few applications currently exist and cost-effective solutions have been elusive because of serious technical and business hurdles. RFID reduces the risk of human error, provides instant stock levels, and can be tied to back-end systems, initiating orders automatically when stock starts to run low. The SMART team has been working to make RFID reliable and more cost effective, and to adapt the technology for use with meat products and in cold storage. The SMART project also worked on developing back-office functions and Web services so the retailer could, for example, automatically relay stock levels to a supplier. The project is scheduled to start testing an RFID system in October 2008, including stock tracking and activity monitoring for promoted goods. SMART's work will make it easier for other projects to design a functioning system and could help propel RFID systems into the retail mainstream.