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

Δελτίο 19
8 Απρίλη 2006

MIT Researchers Attack Wireless Shortcomings, Phishing
Network World (04/04/06), B. Brown

MIT faculty members are pitching their latest research to university partners in the business community at this week's MIT Information Technology Conference. Assistant professor D. Katabi, of the school's electrical engineering and computer science department, presented her research in opportunistic coding, or COPE, to enhance the performance of wireless networks. Katabi says that with demand for wireless throughput increasing steadily, a major breakthrough is needed, one that would go well beyond the next 802.11 iteration. "We need a severalfold increase" in throughput, she said. To accomplish this, Katabi says that systems must take advantage of the shared nature of wireless networks, rather than forcing them into a point-to-point mode. In her system, routers would handle the mixing or coding of packets, and then relay them to senders and receivers that can determine whether the traffic is directed toward them. Katabi reports throughput increases of up to fourfold using this technique in a three-floor MIT building containing 34 nodes. Assistant professor R. Miller described his research on anti-phishing techniques. Miller wants to give browsers the ability to understand their users' intentions, so they could confirm that a URL is the user's intended destination and legitimate. Miller outlined his vision for the Web wallet, a suite of network security features that presents the user with a list of suggested sites with similar URLs to visit, and a separate form to enter his personal information. Miller found in experiments that the wallet dramatically reduced the percentage of users who fell for phishing scams.

The Lessons of the $100 Laptop
eWeek (04/04/06), J. Spooner

Speaking at the LinuxWorld convention, One Laptop Per Child Chairman N. Negroponte said the company is poised to ship between 5 million and 10 million devices by the end of the year or the beginning of next. The computer, equipped with a seven-inch screen, a 500 MHz AMD processor, and a Linux operating system, but shed of its hand crank, will be primarily used as an educational tool, teaching children in developing countries to write computer programs and enabling them to connect to the Internet. In outlining the progress of the laptop, Negroponte was sharply critical of the computing industry's cycle of software updates that add features but not value, arguing that the industry needs to re-evaluate its approach to development. The laptop sheds the costs of a proprietary operating system, a large display, and sales and marketing support, while still being readable and capable of connecting to the Internet, as well as serving as a router for other machines. Energy consumption was a major concern in developing the laptop, and Negroponte boasted that the device will consume fewer than 2 watts of power. "That's very important because 35% of the world doesn't have electricity," he said, adding that companies will routinely boast of the efficiency of their products in the near future. "That is the currency of tomorrow." The laptops will also contain Wi-Fi mesh networking capabilities that work even when the machines are powered down, enabling multiple machines to use the same Internet connection. The hand crank will move to the device's power supply.

US Takes Interest in DDoS Attacks
Computer Business Review (04/03/06), K. Murphy

Recent distributed denial-of-service (DDoS) attacks targeting the Internet's domain name system (DNS) have attracted the attention of high-level officials in the U.S. government, who fear that a new technique enabling attack authors to direct far more traffic at their victims could suggest the work of a new breed of cyber criminal motivated by the desire to bring down the Internet altogether. The alarming series of DNS amplification attacks began in December and rose appreciably in February, using spoofed IP addresses and recursion to broaden the scope of attacks. Traditional DDoS attacks use botnets either recruited through spammed Trojans or worms or purchased on the black market, often sufficient to overwhelm smaller sites, but the amplification attacks use a much larger network to target large companies or critical elements of the DNS infrastructure, such as the .com registry. "We're seeing some very deliberate attacks against some high profile targets right now, to showcase the talent of the attacker, so they can get work for the Russian mafia or whoever it may be," said Internet Systems Consortium President P. Vixie. The ease with which a home PC can spoof its IP address when sending out a packet enables these attacks, provided the author obtains control of a DNS record. The attacker then instructs the bots to issue requests for a particular piece of malware against open recursive name servers. About 50,000 recursive name servers were used in the recent attacks, estimates CTO of UltraDNS Rodney Joffe, who was recently called away from a presentation at an ICANN meeting to brief top U.S. officials. UltraDNS and VeriSign were both targeted in recent attacks. Experts are debating whether the attacks originate from hackers looking for recruitment or terrorists more concerned with the wholesale disruption of economies. Vixie and ICANN agree that the most effective prevention against such attacks would be for ISPs to routinely validate source IPs.

Your Secrets Are Safe with Quasar Encryption
New Scientist (03/29/06), W. Knight

Japanese scientists have encrypted messages using quasars, which emit powerful radio waves and are believed to be produced by black holes. K. Umeno and colleagues at the National Institute of Information and Communications Technology in Tokyo believe the intergalactic radio signals of quasars have the potential to serve as a cryptographic tool because their strength and frequency make them impossible to determine. "Quasar-based cryptography is based on a physical fact that such a space signal is random and has a very broad frequency spectrum," says Umeno. The researchers view quasar radio signals as a way to create genuine randomness when encrypting information at high speed, and make it easier for two communicating parties to securely share the source of randomness. Users of the method only need to know which quasar to target and when to start in order to encrypt and decrypt a message. A large radio antenna is not required, and the parties can be located in different hemispheres. International financial institutions, governments, and embassies would benefit from quasar encryption, says Umeno. However, some observers have concerns about the practicality of the method, which is untested, and may be vulnerable to an attacker who is able to mimic the radio signal.

Building Better Applications: Beyond Secure Coding
Enterprise Systems (03/28/06), M. Schwartz

In the face of mounting security breaches, regulatory requirements, and audits, more companies are working to educate their developers about secure coding, with the goal of creating software with as few vulnerabilities as possible. The premise is that improved training will

lead to applications with secure data encryption, strong passwords, and complete input validation. Bad code accounts for as many as 80% of the security problems in existence today, wrote security consultant B. Biszick-Lockwood in an IEEE report. As part of an IEEE group commissioned to study secure computing, however, Biszick-Lockwood found that most security problems emerge from constrained budgets, unreasonable deadlines, and a lack of support from executives, rather than inadequate training. Bad code is more often indicative of business problems than a flawed development team. The data breach notification emails that customers receive with alarming frequency speak more to a basic misunderstanding of the business value of security at a decision-maker level than to an error in a specific application. Executive education is the first place to start when trying to develop a culture of secure computing, says H. Thompson of Security Innovation. Since selling executives on the value of an education program can be tough, developers can use a calculus that identifies potential flaws at each stage of development, weighing the cost of fixing bad code before it is released compared with fixing it after the release. With senior management on board, development teams must then adjust their thinking to account for what constraints need to be built into the application from the outset, rather than simply focusing on the application's core functionality. Once a project is completed, companies must subject their code to rigorous security testing just as they test for functionality, attacking it as a hacker would.

An Image of the Future: Graphical Passwords
Information Today (03/06) Vol. 23, No. 3, P. 39; D. Poulson

Computer users frustrated with having to remember a multitude of alphanumeric passwords will welcome the development of graphical passwords, writes D. Poulson. First patented by physicist and entrepreneur G. Blonder in 1996, graphical passwords work by displaying an image on a touch-screen or pen-based computer, and prompting the user to select the areas in the image, called click points, that form a password. To work, the image must be sufficiently complex, such as a city skyline, and users must be on the lookout for password thieves trying to shoulder surf, or steal a password by observing the click points, just as thieves observe keystrokes to steal conventional passwords. But researchers at the University of Rutgers are developing a graphical password that is invulnerable to shoulder surfing. In their tests, users chose 10 icons from a pre-selected list, which were then mixed up on the screen with 200 other icons. Rather than clicking on the icons themselves, the subjects clicked inside the geometric shape that would be formed by lines drawn to connect the icons. Correctly identifying 10 shapes validates the user. Shoulder surfing becomes impossible when a user never clicks on the actual icons, said Rutgers computer science professor J.-C. Birget. The problem with the icon-based password is that it takes too long, due to the multiple rounds of selecting icons. Though Birget believes icon-based passwords may only be used in environments where shoulder surfing is a serious problem, he said test subjects in his experiments did not notice the extra time required to select the icons.

To Packed Crowd, Speaker Discusses Cyber Security Crisis
The Spectrum (04/07/2006), T. Halleck

Speaking at the University at Buffalo, cyber-security expert Eugene Spafford criticized the government and private industry for a haphazard approach to combating cyber crime. "We have people committing (cyber crime) offenses again and again, but it's been calculated as less than five percent of these crimes are prosecuted," Spafford said. Often the victims of cyber crime are large companies reluctant to disclose that their security has been compromised, while law enforcement in the area of computer crime is still in its infancy. A major US Army

command center recently scrapped all of its computers because of pervasive security problems. It invested in a new, $36 million system that was reportedly compromised in three weeks, Spafford said. While serving on the President's Information Technology Advisory Committee (PITAC), Spafford realized that no one was adequately addressing the problem of cyber security. "What is Congress doing? They're stopping research and development spending. The amount the PITAC asked for was an estimated $100 million a year. The US spends that much in three days in military operations in Iraq." While the government's response to cyber crime has been lackluster, Spafford takes heart in the growing interest in security among academic researchers. He also notes that public awareness of the problem is slowly beginning to spread, though people continue to respond to unsolicited email asking for personal information.

A Pretty Good Way to Foil the NSA
Wired News (04/03/06), R. Singel

P. Zimmerman, author of the PGP email encryption program, has developed an open-source software application to secure Internet phone calls. Zfone is currently only available for OS X and Linux, though a version for Windows is expected this month. The program encrypts and decrypts voice calls as traffic moves in and out of the computer, and does not require users to predetermine an encryption key or enter lengthy passwords. Zfone, which has already been tested with X-lite, Free World Dialup, and the Gizmo Project, is intended to be compatible with any VoIP client using the standard industry SIP protocol. During the call, the software displays a three-character code for each caller to read aloud to defend against man-in-the-middle attacks, where eavesdroppers intercept the cryptographic keys between two callers. If someone is attempting to intercept the communications, the spoken codes will not match what appears on the callers' screens, and they will know that someone is attempting to listen in. Zfone is based on the SRTP system that adds a 3,000-bit key exchange to the 256-bit AES cipher to generate the three-character codes that users read aloud to each other. The protocol has been submitted to the IETF for standardization. Zfone is intended principally to compete with Skype's proprietary encryption system, which is not available for peer review and is alleged to contain demonstrated vulnerabilities.

Beat Cybercrime, Switch to a Virtual Wallet
New Scientist (04/01/06) Vol. 190, No. 2545, P. 28; C. Biever

To simplify the process of conducting online transactions, Microsoft is promoting the concept of a virtual wallet, a collection of icons on various Web sites that users can click to verify their age, billing information, or other personal details without having to remember multiple user names and passwords. The system should also improve security by eliminating easily hacked passwords and subjecting common Internet transactions to the same cryptographic protocols used in banking and government. "From a user standpoint, it's really simple, it's fast, and it's much more secure," says digital identity expert D. Reed. Microsoft intends to include the required software in its next version of Windows, while the Eclipse Foundation is developing a similar application for Apple and Linux systems. The Internet was not built with the idea in mind that people would have to verify each other's identity, and passwords have proven too easy for hackers to crack. Microsoft's earlier attempt at a universal verification scheme, Passport, failed amid concerns that the company would act as the custodian for every consumer's identifying information. Credit card companies and other third parties are responsible for guarding information in Microsoft's new system, just as they are now. After a user registers, the third party furnishes the Web sites with a digital certificate and the user

with a virtual card that enables him to obtain a digitally signed certificate to proof his identity whenever necessary. Users access the system, which creates public and private encryption keys, with a master password that never leaves a secure section of the computer. The system will not permit users to enter sensitive information on sites that it suspects are spoofed. By requesting the user's computer to decrypt information with its private key, the card issuer creates a digital certificate, which it signs with a digital signature and relays back to the authenticated site.