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

Δελτίο 134
10 Νοέμβρη 2008

A Picture Is Worth a Thousand Locksmiths
UCSD News (10/29/08), D. Kane

University of California, San Diego (UCSD) computer scientists have developed software that can duplicate a key using only a photograph of the key. A key's bumps and depressions represent a numeric code that describes how to open the key's corresponding lock. "We built our key duplication software system to show people that their keys are not inherently secret," says UCSD professor S. Savage. "Perhaps this was once a reasonable assumption, but advances in digital imaging and optics have made it easy to duplicate someone's keys from a distance without them even noticing." Savage presented the research at ACM's Conference on Communications and Computer Security, which takes place Oct. 27-31 in Alexandria, Virginia. In one demonstration of the new software, the researchers took pictures of a residential house key with a cell phone camera and ran the image through their software, producing the information needed to create identical copies. In another demonstration, the researchers used a five-inch telephoto lens to take pictures of keys sitting on a cafe table from more than 200 feet away. Savage notes that locksmiths and lock vendors have been able to copy keys by hand from high-resolution photographs for some time. However, the threat has reached a new level, with cheap image sensors making digital cameras readily available, and basic computer vision techniques are able to automatically extract a key's information without requiring any expertise.

E-Voting Groups Are Watching a Handful of States
IDG News Service (11/02/08), G. Gross

Several US states, including Virginia and Pennsylvania, will be watched closely on election day for problems with electronic-voting equipment, says Verified Voting president P. Smith. She says expected long lines and the lack of early voting options in some states could be problematic if there is any kind of equipment breakdown. "This is an election that will sort of stress-test the [election] systems," she says. "Any problem that's going to come up is going to be amplified." Several states have already reported long lines during early voting, and other states do not have adequate numbers of voting machines available to replace malfunctioning equipment. The problem will be most severe in states with touch-screen machines, such as Pennsylvania and Virginia. In addition to not having early voting, Pennsylvania and Virginia do not require paper-trail backups. Meanwhile, University of South Alabama professor A. Yasinsac will closely monitor Florida and Ohio, as both states have a history of tight races and voting equipment problems. Florida has scrapped most of its touch-screen e-voting machines in favor of an optical-scan system in which paper ballots are scanned electronically. Ohio has faced problems with its e-voting machines during the 2004 presidential election and a primary election this year. Like Florida, Ohio has switched from touch-screen machines to optical-scan systems. Yasinsac, who serves on ACM's voting subcommittee, says that regularly switching between voting machines creates the potential for problems, as there is not enough time to train workers or test the systems. Other states to watch include Maryland, New Jersey, Delaware, Louisiana, Georgia, and South Carolina, all of which use touch-screen voting machines without paper-trail backups.

Scientists Crack Possible Future Quantum Computer Age Encryption
TG Daily (11/03/08), W. Gruener

A system that was considered to be strong enough for quantum computing has been cracked by researchers at Eindhoven University of Technology in the Netherlands. The team built software that is capable of speeding up attacks on McEliece, a 30-year-old public-key encryption algorithm, and used a cluster of 200 computers to decrypt a ciphertext in just one week. Still, the McEliece cryptosystem could be used with more powerful computers because larger key sizes can be scaled to guard against such attacks. The superior strength and scalability of the system has not led to substantial acceptance of the technology in the cryptographic community. The McEliece cryptosystem has a very large public key (219 bits). Encrypted messages are much larger than the plain-text message, which increases the chance of transmission errors. Also, it is an asymmetric key algorithm and cannot be used for authentication or signature schemes.

IBM Researchers Show Off New Weapon in Fight Against Online Fraud
eWeek (10/29/08), B. Prince

A new device devised by IBM researchers is designed to curb the compromising of online banking transactions by man-in-the-middle attacks and malware-infected PCs through the establishment of a direct, secure communications channel to online banking servers. The Zone Trusted Information Channel (ZTIC) can interface with the USB port of any computer to set up the server link, effectively circumventing the user's PC. If the PC is tainted with malware, the user can terminate the transaction while it is displayed on the ZTIC device. Man-in-the-middle attacks are countered because the device encrypts the data and uses its own hardware to carry out authentication and confirmation of the transaction, says IBM's G. Ollmann. "The various phases of the validation and acceptance of a transaction are moved from the PC over to the ZTIC," he says, adding that the system "can use bank-supplied smart-card technologies to further boost this encryption/security." IBM says pilot ZTIC devices are ready for trial. "In the presence of an ever-more professionally operating e-crime scene, it became obvious that PC software-based authentication solutions were potentially vulnerable and that we needed to innovate to stay ahead," says P. Buhler with IBM's Zurich Research Lab. "That was the starting point for developing the ZTIC."

On Security, Microsoft Reports Progress and Alarm
New York Times (11/03/08) P. B9; J. Markoff

The security of the Windows operating system has significantly improved, but the threat of computer viruses, fraud, and other online threats has become far more serious, concludes Microsoft's biannual "Security Intelligence Report." Microsoft blames organized crime, naive users, and its competitors for the deteriorating situation. Microsoft reports that the amount of malicious or potentially harmful software removed from Windows computers increased by 43% during the first half of 2008. The report also says that improved Windows security caused attackers to shift their attention to security holes in individual programs. For example, the report notes that 90% of newly reported vulnerabilities involved applications in the first half of 2008, while only 10% of new vulnerabilities involved operating systems. Microsoft says that software practices must change industry wide otherwise the improvements in Windows will be meaningless. Security researchers agree. "The only thing that Microsoft can patch is their own software," says F-Secure chief security advisor P. Runald. "That's not what the bad

guys are using to get into computers these days. It's certainly a challenge." The computer security industry has been fighting a losing battle as computer criminals are increasingly able to profit from identity theft and a variety of other scams. Microsoft has tried to combat the problem by building a variety of safeguards into its operating systems and its Internet Explorer browser, with mixed success. The Microsoft report notes that the infected rate of US computers rose 25% in the last six months.

Optical Firewall Aims to Clear Internet Security Bottlenecks
ICT Results (10/29/08)

Researchers working on the European Union-funded WISDOM project have developed a firewall capable of analyzing data on fiber-optic networks at speeds of 40 gigabits per second. As demand for data-intensive services increases, telecommunications providers are expanding fiber-optic networks, and while performance has improved, the electronic processes and algorithms used to filter data for security threats is struggling to keep up. Using custom algorithms, WISDOM's optical firewall looks for patterns in the header content of data packets to isolate possible viruses, attacks, and other threats. The WISDOM firewall acts as a primary, high-speed filter that routes suspect packets to electronic processes for additional analysis. The WISDOM firewall was built using an integrated photonic technology platform in which silica-on-silicon circuits form an optical equivalent of an electronic printed circuit board. WISDOM researchers say the hybrid boards can be fitted for components for a variety of uses, including sensor systems, avionics, data transmission, optical processing, and network security.

Board Urges Full Funding of Cybersecurity Initiative
NextGov.com (11/05/08), B. Brewin

A new US Dept. of Defense Science Board report warned the incoming administration of President-elect B. Obama to take steps to protect the nation's information infrastructure, which it said remains vulnerable to attack. The report contained a number of recommendations for how the Obama administration could improve cybersecurity, including placing the "highest priority" on the National Cybersecurity Initiative that the Bush administration implemented in January. The report said the Obama administration should fully fund the initiative and give it "highly focused and frequent management attention to ensure that agreed goals are met with the highest sense of urgency." The report also recommended that the cybersecurity initiative be expanded to protect the commercial information infrastructure used by the finance, transportation, manufacturing, and agriculture sectors. In addition, the report called on the Defense Department to prevent employees and contractors from hacking into or stealing data from information systems by aggressively auditing users who access its computer networks. Finally, the report urged the incoming administration to prepare for a long-term effort to protect against cyberthreats--an effort that will include repeated cycles of computer system testing, vulnerability identification, and application of new defensive strategies.