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

Δελτίο 88
31 Αυγούστου 2007

Computing Breakthrough Could Elevate Security to Unprecedented Levels
University of Michigan News Service (08/16/07), C. Rabuck; N. Moore

University of Michigan researchers have found that pulses of light can be used to dramatically accelerate quantum computers, a breakthrough that could lead to stronger information security and the ability to quickly decipher hacker encryption codes. Working with researchers from the University of California-San Diego and the Naval Research Laboratory, the researchers used short, coherent pulses of light to create light-matter interactions in quantum dots, particles so small that their properties can be altered by adding or removing electrons. University of Michigan professor D. Steel says the researchers found they could control the frequency and phase shifts in the optical network, a crucial aspect of powering an optically-driven quantum computer. Such a computer would take only a few seconds to crack highly encrypted codes that would take today's fastest desktop computers about 20 years to crack. "Quantum computers are capable of massive parallel computations," Steel says. An equally significant aspect of the research is that the technology used by the researchers is relatively inexpensive. "We're particularly excited about our findings because they show that we can achieve these results by using quantum dots and readily available, relatively inexpensive optical telecommunications technology to drive quantum computers," Steel says.

'Virtual Sandboxing' Provides Safe Security Testing
Computerworld (08/09/07), M. Hines

The number of threats Internet users have to face continues to grow, but security researchers at the Usenix Security Symposium presented a new process for protecting users with execution-based malware detection. University of Washington graduate student A. Moshchuk demonstrated a tool that uses a "virtual sandbox" to test Web applications for suspicious behavior before allowing the application to reach the end-user browser. Several other techniques have been developed that can protect end-users from vulnerabilities that have not been identified or patched. Virtualization is being adopted by many researchers to identify unknown vulnerabilities, and Moshchuk pointed out a tool created at the University of Washington called SpyProxy. SpyProxy is injected as a virtual machine that sits between an end-user's browser and a Web site to download and test any application the browser is trying to access to catch any potential attacks before they reach the browser. SpyProxy's virtual machine mirrors the browser being used by someone running the tool and renders any page or application that is accessed to see if the URL contains an attack. Moshchuk says SpyProxy can effecttively run and analyze any type of Web page or application in a few seconds to determine if it contains any patterns common in many threats. SpyProxy does have some limitations, as it works more effectively on sites that contain larger volumes of static content, such as text, and sometimes it has difficulty determining when a page has finished loading, which can add to the delay. The University of Washington team says SpyProxy is capable of monitoring multiple users on clusters of workstations, and a single-CPU device can process about 82,000 page requests in one day, which should cover about 800 users per machine. The researchers plan to distribute the SpyProxy program free of charge.

Encrypting the Future
Government Computer News (08/06/07), K. Hickey

Although the cryptographic security standards used in public-key infrastructures, RSA and Diffie-Hellman, have not been cracked, they were introduced in the 1970s and there is growing concern that the standards may soon be outdated. Consequently, the National Security Agency wants to switch cybersecurity to elliptic-curve cryptography (ECC) by 2010, the same year the National Institute of Standards and Technology plans to recommend all government agencies switch to ECC, according to D. George, technology director of the NSA's information assurance directorate. Using current standards requires continually extending the key lengths, which increases processes time and makes it difficult to secure small devices. EEC is a mathematical algorithm that is used to secure data in transit, and because it provides greater security using a smaller key size, it takes less computational time and can be used on smaller devices, like cell phones, wireless devices, and smart cards. S. Kent, chief scientist at BBN Technologies, says to make RSA and Diffie-Hellman keys, which currently can extend up to 1,024 bits, secure for the next 10-20 years the keys would have to at least double in length, and eventually expand up to 4,096 bits. Switching to EEC, however, will require a massive replacement of hardware and software, and with more than a million different pieces of equipment that need to be changed to EEC, it could take the NSA more than 10 years to complete the process. George says the move to ECC is more than just replacing an encryption system, and is actually upgrading the entire communications structure, which the NSA will use to work more closely with other governments, US agencies and departments, first responders, and the private sector. Interoperability is key to the new communication program and the reason behind the Cryptographic Modernization initiative, which was started in 2001 and promotes ECC. Experts agree that there is no new technology comparable to ECC. "ECC is the only impressive thing out there," Kent said. "People don't get excited every time a new thing comes along. We wait several years and let people try to crack it first. ECC definitely passed the test in this regard."

California: The Top to Bottom Review
VoteTrustUSA (08/13/07), B. Simons

On Aug. 3, California Secretary of State D. Bowen announced the decertification of all electronic voting systems evaluated in her Top to Bottom review, writes former ACM president and League of Women Voters member B. Simons. All systems but one were conditionally recertified, but the recertification came with arduous conditions in certain cases. Such conditions include the requirements that only one direct recording electronic (DRE) unit may be employed per polling site on election day or during early voting; all DRE-cast votes must be counted manually using voter verified paper audit trails; software and firmware must be reinstalled on all machines by jurisdictions; and the vendor must foot the bill for any post-election auditing. Bowen also ordered vendors to generate plans for "hardening" their equipment to shield against certain security threats detected by her review. Bowen's decision was based on reports that the systems were highly vulnerable, insecure, and unreliable, and her office also issued an accessibility review study concluding that "the three tested voting systems are all substantially noncompliant when assessed against the requirements of the [Help America Vote Act] and specified in the 2005 VVSG guidelines." Testing and analysis was held up by vendor delays, leading testing teams to complain that they did not have enough time to sufficiently examine the systems and may have missed other major security holes. Vendors insisted that their voting systems are reliable, secure, accurate, and accessible for all voters, but Simons contends, "It is difficult to imagine that automobile manufacturers, in response to negative crash test results, would argue that their cars would not crash, because safe drivers or good road conditions would prevent such crashes. Yet that is precisely the kind of argument being made by voting machine vendors."

Local Teen Works to Advance Encryption Technology
Henry Herald (08/13/07), J. Jackson

B. Dorminy is still two years away from entering college, but he has already received $40,000 in scholarships, including a $10,000 scholarship from the Davidson Fellows Scholarship Program for his research and presentation on "Improper Fractional Base Encryption," new encryption software that uses the concepts of improper fractional bases. By using reduced redundancy representations of improper fractional bases, Dorminy created a more secure encryption system that requires less computer memory and uses both confusion and diffusion to protect data. Improper Fractional Base Encryption is the first secure method of encryption using improper fractional bases that allows a second message to be stored undetectably within the body of a main message. This year alone, Dorminy has received numerous scholarships, honors, and awards, including the Scientific Depth and Rigor scholarship from Alcatel-Lucent, a perfect score on the 2007 American Mathematics Competition 10.

E-Voting Predicament: Not-So-Secret Ballots
CNet (08/20/07), Δ. McCullagh; A. Broache

Ohio's open-record laws, combined with the paper trails provided by Election Systems and Software voting machines, makes it possible to reconstruct when and how individuals voted, two Ohio activists discovered. Two documents, a list of voters in the order they voted and a time-stamped list of actual votes, can be acquired and combined by anyone interested. Privacy activist J. Moyer and fellow activist J. Cropcho were able to reconstruct the voting results, including how individuals voted, for a May 2006 vote in Delaware County, Ohio, to extend a property tax to fund mental retardation services. "I think it's a serious compromise," says Stanford University computer science professor D. Dill. "We have a system that's very much based on secret ballots. If you have something where voters are involuntarily revealing their votes, it's a very bad practice." P. Gallaway, communications director for Ohio Secretary of State J. Brunner, says Brunner is already planning a "comprehensive" review of e-voting machines as part of a pledge she made during her campaign. Now the review will likely include a look at the ES&S privacy issue as well. ES&S spokeswoman J. Friedman-Wilson downplayed concerns over ES&S privacy and says it would be very difficult to make a connection between the sign-in order and the voting timestamp, adding that Moyer's and Cropcho's analysis is "fatally flawed" because it does not account for time delays between signing in and casting a vote. Computer scientists say restricting the public's access to time-stamped e-voting paper trails is insufficient, and suggest deleting the time stamp, not keeping a record for what order people voted in, and adding a paper cutter and shuffler to randomize how the physical audit trail is recorded.

Voting Machine Hackers--UCSB Team Breaks Into Counting Device
Pacific Coast Business Times (08/16/07), S. Nellis

California Secretary of State D. Bowen was eventually persuaded to ban the use of an electronic voting machine in state elections by a successful attempt to hack the system by a team of University of California, Santa Barbara computer scientists. The team of hackers demonstrated that with enough know-how, dedicated attackers could compromise e-voting systems and fix elections. The machine the UCSB team tested was manufactured by Sequoia, and the researchers ascertained that the device was both physically and electronically exploitable. UCSB professor R. Kemmerer said crafting the malicious software to infect the system would take considerable skill, but very little training was necessary to launch the hacks. He added that the team was able to compromise the voting system without access to source code. UCSB doctoral student W. Robertson noted that while access to the central vote-counting server is supposed to be closely guarded, "in practice, it's often the case that isn't observed." The hackers also discovered that they could modify the machines by swapping initialization cartridges with bogus cartridges without breaching seals on the edges. Not even Sequoia's recommended security protocols prevented the team from cracking the e-voting system. UCSB computer science professor G. Vigna observed that such election tampering would not be detectable even with California's mandatory paper trail.

New URI Browser Flaws Worse Than First Thought
IDG News Service (08/15/07), R. McMillan

Security researchers B. Rios and N. McFetters say they have found a flaw in Windows' Uniform Resource Identifier (URI) protocol handler technology that would allow an attacker to run unauthorized software on a victim's PC and to steal data from the computer. Rios and McFetters call such an attack a "functionality-based exploitation" because attackers simply misuse the legitimate features of software that is launched by the URI protocol handler. "It is possible through the URI to actually steal content form the user's machine and upload that content to a remote server of the attacker's choice," says McFetters. "This is all through functionality that the application provides." Rios and McFetters will not name the company responsible for the software, though they do plan on releasing the results of their research once the vendor has had a chance to fix the problem. Functionality-based exploitations may be the beginning of a new era of problems that are only just starting to be examined by security professionals. "It's a hacker's dream and programmer's nightmare," says Shavlik Technologies chief security architect E. Schultze. "I think over the next six to nine months, hackers are going to find lots of ways to exploit standard applications to do nonstandard functions." Software developers released URI protocol names so users could launch programs from a browser, but they did not properly explore how they could be misused by attackers, McFetters says. Microsoft is working to educate users and developers about URI security problems, but Microsoft security program manager M. Griesi says there is only so much Microsoft can do and that security is an industry responsibility and individual developers need to be more responsible.

Phishing Researcher 'Targets' the Unsuspecting
Network World (08/13/07) Vol. 24, No. 31, P. 26; J. Brodkin

Indiana University professor and cybersecurity researcher M. Jakobsson launches innocuous attacks on unsuspecting Web surfers as part of an effort to discover what scams people are prey to and determine potential new phishing tactics. He argues that such experiments are valuable in figuring out what phishing countermeasures are and are not effective, and anticipating trends by discovering as-yet unexploited human vulnerabilities. It is critical to Jakobsson's experiments that his research subjects remain unaware of their participation to make the results as authentic as possible. Victims of online attacks frequently disclose sensitive information or have their computers hijacked by hackers, and one of Jakobsson's tests revealed that efforts to educate the public about the hazards of online attacks are inadequate. One of his findings indicated that people are willing to respond to bogus emails if the hacker correctly identifies the first four digits of their credit card numbers. In another experiment, in which email addresses were targeted from a social networking site that listed political affiliations, Jakobsson observed that people on the far right and far left were more susceptible to phishing emails than people in the middle. Some of the people and institutions Jakobsson has used as guinea pigs, such as eBay, appreciate the insights he has uncovered and applied them toward the improvement of their security protocols. Jakobsson and colleagues also launched a phishing attack on unsuspecting students at IU.

Can a Government Remotely Detect a Terrorist's Thoughts?
New Scientist (08/11/07) Vol. 195, No. 2616, P. 24; P. Marks

The US Homeland Security Department's Project Hostile Intent (PHI) has the ambitious goal of projecting "current or future hostile intentions" among the 400 million people who enter the country each year through remote behavior analysis systems, according to DHS representative L. Orluskie. He explains that PHI intends to identify physical markers (blood pressure, heartbeat, facial expressions, etc.) associated with hostility or the desire to deceive, and apply this knowledge toward the development of "real-time, culturally independent, non-invasive sensors" and software that can spot such behaviors. Such sensors could include infrared light, heart rate and respiration sensors, eye tracking, laser, audio, and video. For four years, the US Transportation Security Administration has been using the Screening Passengers through Observation Techniques (SPOT) program to detect suspicious people through study of micro-expressions--involuntary facial telltales that indicate attempts to deceive--but the process is costly and arduous, and is not something a baggage screener or customs official can do in addition to their regular duties. The automation of the SPOT program, with computers instead of people screening for micro-expressions and other suspicious bodily indicators, is the impetus behind PHI. Experts doubt that such capability could be accomplished by the end of the decade, if at all, and are skeptical that such systems could identify hostile micro-expressions in a potential terrorist, given the lack of knowledge about and complexity of such expressions. Another unknown factor is whether such signs could be spotted hours or even weeks before a terrorist incident. There is also the danger that innocents who are highly emotional or aggravated due to stress might be flagged as potential terrorists.