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

Δελτίο 39
11 Σεπτέμβρη 2006

"'Molecular Computers' Act as Tiny ID Tags"
New Scientist (09/03/06); K. Kleiner

Researchers have developed molecules with the ability to perform rudimentary logic operations, potentially functioning as tiny identification tags for cells or nano-devices. The idea was born from research conducted at Queen's University in Belfast, that focused on molecules that emulate the behavior of silicon logic gates. As an input, the molecules use a chemical or a mix of chemicals, with light as an output. Research in molecular computation holds the potential to perform billions of calculations simultaneously, although it has thus far proven difficult to piece together the simple operations required to enable complex functionality. In search of a more immediate use for computational molecules, Queen's University's Prasanna de Silva developed a technique to use them as molecular tags, which are similar to RFID tags, only smaller. De Silva's technique could eventually be automated, with individual cells tagged with a sequence of figures such as a license plate number. "What really makes the numbers go through the roof is combining operations," De Silva said. The process can be streamlined by combining the logical functions so that a large group of tags can be produced that each provides a different answer. Medical researchers could ultimately use the research to tag and isolate individual cells. "The study shows that molecular computation can indeed find real applications today," said University of Bologna chemist V. Balzani.

"University Research Aims at More Secure Wi-Fi"
InformationWeek (09/01/06); J. Shandle

Researchers at Carleton University in Canada continue to improve signal fingerprinting technology that has the potential to serve as a solution for protecting wireless networks from unauthorized users. The signal fingerprinting technology makes use of the RF signal fingerprints or profiles, which differentiate wireless transceivers. J. Hall, a graduate student who is heading the research initiative, says the unique fingerprint characteristics are the result of the differences in silicon and other electronic components of wireless transceivers, particularly the variations in transient signals when the transceiver tries to connect to the network. The fingerprint is compared to authentic versions stored in the access point or another central location in the network using a probabilistic neural network. For example, RF fingerprinting would be able to reveal when a hacker has tried to use a spoofing technique to give a transceiver a specific MAC address. Self-organizing map technology and clustering technology could be used to ease storage of authenticated signatures and make authentication faster. The researchers also plan to use a DSP-based data acquisition board to pick up transient RF signals rather than Anritsu's Signature High Performance Signal Analyzer. Scalability and effectiveness of algorithms are issues that still need to be addressed before the Carleton team moves forward with any commercial aspirations.

"Stealth Attack Drains Cell Phone Batteries"
UC Davis News and Information (08/24/06)

Cell phones capable of transmitting or receiving multimedia files could be the target of an attack that surreptitiously drains their battery power, according to computer security researchers at the University of California, Davis. "Battery power is the bottleneck for a cell phone," said H. Chen, assistant professor of computer science at UC Davis. "It can't do anything with a dead battery." By spending most of their time in standby mode, cell phones are designed to conserve battery power. The MMS protocol, which enables cell phones to transmit media files, can be used to send packets of unwanted information to a cell phone, waking the device from standby mode. The cell phone promptly discards the junk packets without alerting the user. Repeated reception of junk data keeps the device in active mode, running down the phone's batteries as much as 20 times faster than normal use. All an attacker would need to know, Chen says, is the phone number and Internet address of the victim's cell phone. Chen and his graduate students have discovered other flaws in the MMS protocol, including one that would enable users to send multimedia files for free by circumventing the billing processes for multimedia services.

"The Non-Denial of the Non-Self"
Economist (08/31/06) Vol. 380, No. 8493, P. 72

Taking a cue from the philosopher Carl Hempel, who in the 1940s demonstrated that the logical statement "all ravens are black" could be manipulated to form the equivalent "all non-black objects are non-ravens," computer scientists are looking to apply similar negative representations to secure sensitive data by creating a database that contains everything in a particular set of things but the information of interest. The idea of the negative database, whose leading researcher is Yale University computer scientist F. Esponda, materialized a couple years ago when Esponda was studying the human immune system. In that case, "everything" refers to the set of potential biological molecules. The immune system can guard against pathogens without knowing what the pathogen might look like. Rather, it uses a negative database to identify which pathogen it needs to destroy. The immune system knows which biological molecules are "self," for common parts of the body that it is protecting, so when a "not-self" molecule appears, it assumes that it is part of a pathogen and destroys it. The correlation to computer databases is imperfect, as the number of biomolecules, though very large, is not infinite. But by defining "everything" as a finite group, such as phrases with a set maximum number of characters, the technique could be used to compile a database containing names, addresses, and Social Security numbers, for instance. While it would not promise perfect security, the technique could be used to guard against phishing ventures that might, for instance, troll for all the Social Security numbers of the people who live on a particular street. Esponda points to the technique's potential to shore up applications where multiple datasets with different owners need to be compared, providing an effective backup to traditional cryptography.

A Report Card on Anti-Terror Technology
CNet (09/07/06), D. McCullagh

While the federal government has developed and adopted many anti-terrorism technologies in the five years since the Sept. 11, 2001, attacks, the FBI is still working with out-of-date computer systems, the Dept. of Homeland Security is struggling to systemize its container inspections, and it remains uncertain whether the passports with RFID tags that are being rolled out are any harder to duplicate. The FBI has only recently launched an initiative to outfit its field agents with wireless technology to take and upload digital pictures of a suspect that other agents could, in turn, view on their BlackBerry. Preliminary feedback from agents has

been positive, and the FBI hopes soon to roll the system out to all its field offices, though it has not yet established a timetable. The FBI is also behind on search technology. The agency's Investigative Data Warehouse tool, which enables approved users to search through some 650 million records of multiple government agencies through a single Web interface, does not update information in real time, instead waiting for contributing agencies to upload their records into the system. "Right now, we don't have that Google-like search capacity to go (directly) into databases of different agencies," said Z. Azmi, the FBI's CIO. Also, government auditors have declared the computerized modeling system designed to help identify which cargo containers should be inspected a failure. Government intelligence could also benefit greatly from improved language-translation software that can provide automatic real-time translations of obscure languages such as Pashtu and Somali. While many of the government's post-9/11 technology initiatives lag frustratingly behind schedule, others have raised troubling privacy questions, such as the proliferation of surveillance cameras in public places, particularly if they were to be used in conjunction with facial recognition software. Another potentially invasive technology is known as brain fingerprinting, which relies on the detection of an electrical signal to try to determine whether a suspect was present at a crime scene, which has already been ruled admissible by one judge in Iowa.

Researchers Challenge DOS Attack Data
Dark Reading (09/06/06), T. Wilson

A group of University of Michigan, Carnegie Mellon University, and AT&T Labs-Research researchers say DOS attack data may not be generated by sources of spoofed IP addresses as previously thought. The researchers conducted a study that found 70% of DOS attacks are created by less than 50 sources. Many think IP spoofing is the most popular way to launch a DOS attack, but the researchers found that IP spoofing was found in a only a small number of incidents. Unwanted traffic that is delivered to unused addresses, commonly known as backscatter, is often used as a way to track DOS attacks, but researchers say it does not track DOS attacks launched by botnets. The report found that <1% of directly measured attacks produced backscatter. The researchers suggest that organizations use DOS defense tools to decrease the number of malicious traffic.

U.S. Leadership on Cybersecurity 'AWOL'
SD Times (09/01/06)No. 157, P. 1; deJong, Jennifer

For nearly two years, the position of cybersecurity chief at the Dept. of Homeland Security has been vacant, and while the department could be close to appointing an acting assistant secretary for cybersecurity and telecommunications, such a move would be little more than a stopgap. "We are operating without a cyberspace czar," said R. Moritz, chief security officer at CA, noting that government and industry will never be in a full partnership until a permanent appointment is made. Chief among the security concerns is the increasing frequency of consumer-data breaches. The absence of leadership has also stalled the department's response to the recommendations on creating secure software drafted by the Improving Security Across the Software Development Lifecycle task force, which Moritz co-chaired. "It is frustrating not having the government respond to that," he said. In 2003, DHS brought in Symantec executive A. Yoran to lead its cybersecurity branch, but he resigned after just a year. Though Yoran has not made his reasons for leaving public, it has been reported that he was given less authority than promised at the department. While it continues the search for a nominee, DHS has launched the "Build Security In" Web portal to provide guidance to software developers, and in the future it will sponsor publications that support software security.

Sandia's Red Teams: On the Hunt for Security Holes
eWeek (09/04/06) Vol. 23, No. 35, P. 22; C. Preimesberger

Countries and companies hire Sandia National Laboratories' Red Teams to project and assess cyber-terrorism scenarios, produce worst-case contingency measures, and deter a pending attack by patching existing vulnerabilities. "The threat and risk level has never been higher for cyber-security," maintains Red Teams' leader M. Skroch, who says government agencies and utilities' replacement of custom IT systems with cheaper, commercially available Windows and Unix systems places them at greater risk because the off-the-shelf components are more hackable. Each Red Team consists of a small group of computer and systems experts who supply independent evaluations of information, communication, and critical infrastructure to spot security holes, upgrade system design, and help decision makers boost system security. "We have a spectrum of assessment methodologies and assessment types that we apply as needed to most efficiently meet customer goals and provide consistent, measurable and actionable results," explains Skroch. Sandia's Information Operations Red Team and Assessments (IORTA) group lists 8 "red teaming" categories--design assurance, hypothesis testing, benchmarking, behavioral red teaming, gaming, operational red teaming, penetration testing, and analytic red teaming--that are blended together to fuel evaluations. In addition, the teams employ external methods such as event trees and fault trees, processes such as the Control Objectives for Information and related Technology governance framework, and open-source computer and network security tools that apply to specific assessments. Both hardware and software tools are used by IORTA, with Skroch noting that some tools are utilized in an analytical capacity, others are used for planning attacks, and still others are used to make contact with targets. According to him, the Red Teams also create their own scripts and tools on the spur of the moment.

Spam+Blogs=Trouble
Wired (09/06) Vol. 14, No. 9, P. 104; C. Mann

Spam blogging or "splogging" is the practice of posting nonsensical gibberish in blog form and then getting viewers to click on ads that run next to the text, and Wired contributing editor C. Mann warns that the Internet's potential as a user-controlled, bottom-up platform for all kinds of data could be undone by such chicanery. Splogs are created by software that pillages Web pages for potential search terms, automatically copying text and then jumbling it together, thus creating a deceptive blog that searchers might click on without realizing it is a scam. "The blogosphere is increasingly polluted by spam," reports Six Apart VP A. Dash. Spammers are using blogs as components in fake networks of interconnected sites or "link farms," which are employed to imitate the popularity that search engines use to determine sites' ranking on search results pages. Dash is concerned that as spammers seek easy money through pay-per-click advertising via highly ranked search results, the time will come when there will be "a reckoning with the economy that's building up around search engine rankings, one way or another." Sploggers can not only set up vast numbers of bogus blogs, but can also assume control of abandoned real blogs; worse still, sploggers employ robo-software to inundate real blogs with phony comments that link back to the splog. To spot splogs so they can be eliminated from blog-search companies' results, Technorati founder David Sifry proposes training computers to recognize splog identifiers that are distinct from authentic blog characteristics, while URLs with multiple dashes and .info domains are other splog telltales. Dash thinks the best defense against sploggers is the enforcement of accountability, and Six Apart's solution is to make bloggers pay a monthly fee, which not only ties bloggers to a

bank account but also discourages spammers, who would have to pay outrageous sums to support the massive numbers of splogs they operate; realizing that not all companies will employ such a scheme, Dash suggests the implementation of a global identifier.