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

Δελτίο 175
30 Μάη 2010

Cars' Computer Systems Called at Risk to Hackers
New York Times (05/13/10), J. Markoff

Tomorrow's Internet-connected cars could be vulnerable to hackers in the way computers are today, warn researchers at the University of Washington (UW) and the University of California, San Diego (UCSD). During a recent test, the researchers were able to remotely control a car's braking and other functions. "We demonstrate the ability to adversarially control a wide range of automotive functions and completely ignore driver input--including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on," the researchers write. The researchers were also able to insert malicious software into the car and then erase any evidence of tampering. "Taken together, ubiquitous computer control, distributed internal connectivity, and telematics interfaces increasingly combine to provide an application software platform for external network access," write the researchers.

Physicists Use Location to Guarantee Security of Quantum Messages
Technology Review (05/13/10)

University of California, Los Angeles (UCLA) researchers have developed a type of quantum cryptography, which guarantees that only a person at a certain location can read an encrypted message. The researchers say their method makes no assumption other than that laws of quantum physics are correct. It is not technically complex, because it only calls for a qubit to be sent along a quantum channel, while all other communication can be completed classically. A quantum measurement is required, but not quantum computation. The researchers say that there is no technological reason why this scheme cannot be implemented today. Although the approach is relatively simple, the proof of its security is complex and involved. "Unfortunately we do not have a security proof, and we leave it as an open problem to find an attack or prove its security," says UCLA's N. Chandran.

Feds Seek Game-Changing Cybersecurity R&D
GovInfoSecurity.com (05/13/10)

The White House has identified tailored trustworthy spaces, moving target, and cybereconomic incentives as themes for encouraging future game-changing research and development in cybersecurity for the federal government. In a notice recently published in the Federal Register, the National Coordination Office for the Networking and Information Technology Research and Development Program outlines the three themes and their challenges, including the high cost of securing information infrastructures, an asymmetrical cost of attack that favors attackers, and the lack of meaningful metrics and sound decision-making when allocating security resources. "Achieving enduring trustworthiness of the cyberspace requires new paradigms that re-balance security asymmetries of today's landscape," says the notice. The National Coordination Office is seeking public comment to help refine the themes. For example, the office wants to know how the themes could be enhanced, how organizations would support or incorporate the themes, and whether they can cite any state-of-the-art activities and use cases that support the themes.

History of Social Network Use Reveals Your Identity
New Scientist (05/18/10), J. Giles

Web browsing history can be used to identify individuals in a membership group on a social networking site, according to researchers at the Vienna University of Technology. The researchers built a Web site to read the Web addresses visited by people who use Xing, a business-oriented social network based in Hamburg, Germany. They collected data on 6,500 groups containing 1.8 million users, and analyzed the overlap between the lists of names of group members that were publicly available. The researchers estimate that 42 percent of Xing users could be uniquely identified by the membership groups they visited. Xing has begun to add random numbers to mask addresses, but the response might not be enough to foil a similar snooping site, says Stanford University computer scientist A. Narayanan. The next round of Firefox, Chrome, and Safari browsers could have fixes to prevent browsing history from being relayed to Web site owners.

Risk of Cyberattacks Growing: CSIS Memo
CBC News (Canada) (05/18/10), B. DeCillia

A secret memo from the Canadian Security Intelligence Service (CSIS) warns that the risk of cyberoffensives against government, university, and industrial computer systems has grown significantly over the past year. "In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure, and low-risk means to conduct espionage," the memo says. Canadian government officials say they are developing a framework to manage cyberattacks, yet Canada still has no official coordinated cyberattack response strategy. Meanwhile, a report from the University of Toronto's Citizen Lab, the SecDev Group, and US researchers from the Shadowserver Foundation emphasizes that the federal government must take urgent action or risk being targeted by hackers who steal sensitive information using social media. However, University of Calgary computer science professor J. Aycock warns that the Internet's design makes it difficult to provide complete security. "It's not designed to be able to track people back," Aycock says. "There is no one cure-all."

P2P Networks a Treasure Trove of Leaked Health Care Data, Study Finds
Computerworld (05/17/10), J. Vijayan

Dartmouth College researchers have found that health care data is as easily accessible on peer-to-peer (P2P) networks now as it was before the enactment of a new US data security law last September. The study found that more than 20 percent of the documents researchers discovered after performing keyword searches on P2P networks contained information that would be protected under the law, known as the Health Information Technology for Economic and Clinical Health (HITECH) Act. The study found that much of the sensitive data found on P2P networks - such as insurance information, sensitive patient communications, and personally identifiable information - was contained in insecure spreadsheets and Microsoft Word documents. Dartmouth professor E. Johnson says this indicates that many organizations are not taking steps to adequately protect data as they are required to do under the HITECH Act. The study also found that many organizations were not even aware that they were leaking information over P2P networks, Johnson says.

Cyber Challenge: 10,000 Security Warriors Wanted
Campus Technology (05/14/10), D. Schaffhauser

The goal of the US Cyber Challenge is to recognize and train a cohort of 10,000 cybersecurity experts to help address gaps in government and industry. Program director K. Evans says the concept behind the initiative is to cultivate participant skills and provide access to training and practice. She envisions the challenge possessing three core elements--community building for participants, "rack and stack" for recognizing skills and interests, and matching up individuals with government agencies offering scholarships and industry offering internships and jobs. An alpha run for the Cyber Challenge is being conducted this summer, where participants in California, New York, and Delaware can test a free online treasure hunt developed by the SANS Institute. Successful participants will be invited to attend a summer camp where they will get a week of training by SANS and university faculty and students. At the week's conclusion, participants will be broken up into teams to play a capture-the-flag competition by finding vulnerabilities in their opponents' systems while protecting their own.

Ultra-Secure Quantum Communications
University of New South Wales (05/20/10), P. Trute

University of New South Wales researcher R. Malaney has used a new quantum communication process that enhances the unbreakable encryption security of quantum communication. "Unconditional location verification" limits access to a secure message to a recipient who must be at an agreed upon geographic point. "If they are not at that location the process would detect that and you can stop the communication," Malaney says. "This is a new application that you can deploy on current and emerging quantum networks." The process involves the sending of paired qubits over a fiber-optic or wireless network to a recipient, who must send a return message, using information from the decoded qubits, to several reference points to open up a secure channel. The amount of time it takes to return the message can be accurately measured because quantum networks operate at the speed of light and quantum information cannot be copied. This accurate measurement of return time ensures the message has come from the right place.

Scientist Infects Himself With Computer Virus
Financial Times (05/26/10), M. Palmer

University of Reading scientist M. Gasson has deliberately infected himself with a computer virus in order to study the potential risks of implanting electronic devices in humans. Gasson implanted a radio frequency identification chip into his left hand last year. The chip, which is about the size of a grain of rice, gives him secure access to Reading's buildings and his mobile phone. Gasson then introduced a computer virus into the chip. He says the infected microchip contaminated the system that was used to communicate with it, and notes that it would have infected any other devices it was connected to. Gasson says the experiment provides a "glimpse at the problems of tomorrow," considering devices such as heart pacemakers and cochlear implants are essentially mini-computers that communicate, store, and manipulate data. "This means that, like mainstream computers, they can be infected by viruses and the technology will need to keep pace with this so that implants, including medical devices, can be safely used in the future," he says.

Major Step Ahead for Cryptography
University of Bristol News (05/26/10), J. Fryer

Researchers at the University of Bristol (UB) and Katholieke University have developed a new system for encrypted data computing that they say could have a broad impact on areas such as database access, electronic auctions, and electronic voting. "Our scheme allows for computations to be performed on encrypted data, so it may eventually allow for the creation of systems in which you can store data remotely in a secure manner and still be able to access it," says UB professor N. Smart, who developed the system along with Katholieke's F. Vercauteren. Many encryption schemes have been proposed that either have the "add" operation or the "multiply" operation, but not both. In 2009, IBM researcher C. Gentry developed the first scheme that simultaneously allows users to add and multiply ciphertexts. However, Gentry's scheme was only theoretical. Smart and Vercauteren's scheme is a simpler version of Gentry's scheme. Although the new system is not fully practical, it is a key step toward forming a system which is truly practical.

DARPA Builds Cyber Range to Test Security Measures
Government Computer News (05/24/10), B. Rosenberg

The US Defense Advanced Research Projects Agency (DARPA) is working with industry to develop the National Cyber Range (NCR), a cybersecurity testbed for researching network attack-and-defend strategies on a wide scale. The goal is to accelerate government research and development in high-risk, high-return areas and jumpstart technical cybertransformation in the private sector. NCR will provide a real-world simulation environment that companies and research organizations can use to develop and test advanced concepts and capabilities for defending US communications networks against cyberthreats. "We want to create a test range that is fully automatic and rapidly configured so that we can get the results back out to the community," says DARPA's M. VanPutte. "We need better solutions, so what we ask is for the community to bring their ideas to NCR, test them, and see what works and what doesn't work in a quick fashion." During the second phase of the NCR program, which began in February 2010, DARPA, Lockheed Martin and Johns Hopkins University will build and evaluate prototype ranges and their corresponding technology.

Microsoft Researchers Propose Privacy Sensor 'Widget'
Dark Reading (05/25/10), K. Jackson Higgins

Microsoft researchers have developed a sensor widget concept that issues alerts and lets users control what others see from their webcams, microphones and other live data streams. Microsoft's J. Howell and S. Schechter say their research grew out of concerns that applications are able to access multimedia peripherals even after the user's activities are finished. The researchers envision a sensor tool that provides an animated representation of how an application is gathering the user's data. "The moment the application attempts to access these sensors, three sensor-access widgets will appear within the application, informing the user of the data that is about to be revealed," Schechter says. The researchers recommend a configuration that lets applications access only webcams, microphones, and global positioning systems after users have had time to notice the application is about to gather data from them. "We believe this is an important issue given the emerging class of application platforms that can enforce restrictions on the resources that can be accessed by applications," Schechter says.