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

Δελτίο 159
30 Σεπτέμβρη 2009

Machines Can't Replicate Human Image Recognition--Yet
Penn State Live (09/09/09), J. Spinelle

A Pennsylvania State University (PSU) study found that computers, while catching up to humans in many ways, cannot recognize distorted pictures. PSU professor J. Wang and colleagues tested the differences between the human and machine ability to interpret images. Their purpose was to find better ways to increase Web security by developing online barriers that automatic programs cannot cross. The researchers developed a program called IMAGINATION that uses a visual Completely Automated Public Turing Test to Tell Computers and Humans apart (CAPTCHA) to protect against malevolent robotic programs. In the PSU study, both humans and robotic programs tested IMAGINATION, but only humans were able to recognize distorted pictures. The robotic programs could only identify images when they were part of an accurate picture. Wang hopes that Web sites will eventually use IMAGINATION to increase online security. However, he notes that computers may overcome this handicap in the future. "We are seeing more intelligently designed computer programs that can harness a large volume of online data, much more than a typical human can experience in a lifetime, for knowledge generation and automatic recognition," Wang says. "If certain obstacles, which many believe to be insurmountable, such as scalability and image representation, can be overcome, it is possible that one day machine recognizability can reach that of humans."

AFOSR Funds Super-Fast, Secure Computing
Air Force Print News (DC) (09/08/09), M. Callier

The US Air Force Office of Scientific Research (AFOSR) is supporting University of Michigan (UM) physicists' development of components for quantum computers that will enhance security for data storage and transmission on Air Force systems. UM professor D. Steel and his team initially investigated methods to optically produce and maintain quantum coherence using a single electron or hole in a quantum dot structure. A probable key element for long-term success is sustaining a consistent electrical charge for an extended period of time in a solid-state nanostructure. The researchers' next challenge has been exploring how to manipulate the electrical charge to carry out basic computing tasks, and the team has been better able to control and maintain information through the demonstration of well-defined "spin and phase" quantum properties. The researchers have successfully learned how to optically manipulate and measure the spin of an extra electron in a quantum dot in cooperation with Naval Research Laboratory collaborators. Steel's research has yielded new insights into how spin and phase information is lost and how that loss can be reduced, enabling the research team to demonstrate an increase in quantum storage time. When coupled with ultra-fast laser technology, this boost will support more than 1M quantum operations prior to information loss. "State-of-the-art frequency, stabilized lasers, and the advanced laser control system, developed with AFOSR support, will make optical control possible from this time forth," Steel says.

Surveillance Software Solves Security Snag
University of Adelaide (09/14/09), C. Gibson

University of Adelaide researchers have developed software that eliminates the need for security personnel at large public venues to search for suspicious activity among hundreds of different video screens. The program streamlines the information gathered from thousands of cameras and channels them into a single sensor. The researchers say the program helps prevent data overload in the surveillance network and saves workers time and effort. The software, developed at Adelaide's Australian Centre for Visual Technologies, is being commercialized by Snap Network Video Surveillance. When security personnel find suspicious activity, they can "perform virtual walkthroughs to investigate without risking their personal safety," says Snap co-founder H. Detmold. He says that because the program makes automatic connections between thousands of security cameras, one security operator can simply "follow people throughout the whole network, in real time." Fellow Snap co-founder and Adelaide professor A. van den Hengel says the software can be used for arenas as large as airports and the 2012 London Olympics. Adelaide resarchers will continue to develop the software with Universities in Australia and New Zealand.

EU Funding 'Orwellian' Artificial Intelligence Plan to Monitor Public for 'Abnormal Behavior', Telegraph.co.uk (09/19/09), I. Johnston

The European Union-funded Project Indect is developing software that monitors and processes information collected from Web sites, discussion forums, file servers, peer-to-peer networks and individual computers in an effort to automatically detect threats, abnormal behavior, or violence. The project involves researchers from more than 10 European countries and is part of the EU's effort to expand its role in fighting crime and terrorism and managing migration. Project Indect, which started earlier this year, is developing a platform for the registration and exchange of operational data, multimedia content, intelligent processing of information and automatic detection of threats. Researchers in York University's computer science department say their goal is to develop "computational linguistic techniques for information gathering and learning from the Web." Another EU project, Automatic Detection of Abnormal Behavior and Threats in crowded Spaces (Adabts), aims to develop models of suspicious behavior so that closed-circuit TV and other surveillance methods can be upgraded to automatically detect suspicious behavior. The Adabts system would track individuals in a crowd and analyze their body movements and the pitch of their voice. Adabts project coordinator J. Ahlberg, of the Swedish Defense Research Agency, says the system will make it easier for security personnel to spot problems. However, Open Europe analyst S. Booth says the projects sound "Orwellian" and raise serious questions about individual liberty and rights. "These projects would involve a huge invasion of privacy and citizens need to ask themselves whether the EU should be spending their taxes on them," Booth says.

Controlling the Language of Security
Science Centric (09/19/09)

A security policy specification that guarantees the reliability and availability of home networks has been developed by computer scientists at Kyungpook National University and the Electronics and Telecommunications Research Institute in Korea. "Whenever a new access to the home network is found, it should be able to authenticate and authorize it and enforce the security policy based on rules set by the home administrator," the researchers say. The researchers developed the Home security Description Language (xHDL), which includes the necessary notation for consistently describing and specifying the security policy, and ultimately securing a home network. XHDL consists of a combining-rule element, authentication element, user element, object element, object-group element, role element, and rule elements.

Each term could be used to run a browser-based control center. The domestic administrator would have simple control options for allowing access to the home network for specific devices and for controlling the packets of information that pass through the gateway to and from the Internet. XHDL would protect home networks from cyberattacks and ensure that it is available for use.

UK's Centre for Cyber-Security Opens at Queen's
Queen's University Belfast (09/23/09), L. McElroy

The Centre for Secure Information Technologies (CSIT) recently opened at Queen's University Belfast. CSIT will create 80 new positions and serve as the United Kingdom's primary center for the development of technology to fight malicious cyberattacks. The research conducted at CSIT will help prevent Internet crime and protect the security and trustworthiness of electronically stored information. CSIT is one of the first Innovation and Knowledge Centers established in the UK. The center is backed by funding from the Engineering and Physical Sciences Research Council and the Technology Strategy Board, and more than 20 organizations have committed to supporting CSIT's work over the next five years. CSIT will unite research specialists from fields including data encryption, network security systems, wireless-enabled security systems, and intelligent video analysis. CSIT principal investigator professor J. McCanny believes the new center will become globally recognized thanks to the breadth and depth of its technological capabilities, and because it represents a new international paradigm for innovation.

Ants vs. Worms: Computer Security Mimics Nature
Wake Forest University (09/21/09), E. Frazier

Pacific Northwest National Laboratory (PNNL) researcher G. Fink is working with Wake Forest University professor E. Fulp to develop a computer security program that models itself after the defensive techniques of ants. The new anti-malware system uses itinerant digital ants to find problems in a large network. When an ant comes across something suspicious, it leaves behind a "scent trail" that draws an army of ants to the problem. The large group attracts the attention of computer users to a possible invasion. "Our idea is to deploy 3,000 different types of digital ants, each looking for evidence of a threat," Fulp says. Rather than equipping all digital ants with the same memory-heavy defenses, the program apportions certain threats to specific digital ants. The digital ants report to a "sentinel" located at each computer, which in turn is supervised by a "sergeant" of the network. All sergeants are monitored and controlled by human users. To test the program, the researchers sent a computer worm into the system and the digital ants were able to corner the worm. PNNL has given the researchers more time to study the program. If successful, the researchers say the program would be ideal for universities, government agencies, and corporations that rely on large networks.