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

**Δελτίο 173**
**30 Απρίλη 2010**

## Scientists Work to Keep Hackers Out of Implanted Medical Devices
**CNN (04/16/10), J. Sutter**

Researchers are developing ways to prevent hackers from accessing and remotely controlling medical devices that emit wireless signals. For example, Oak Ridge National Laboratory's N. Paul is designing a more secure insulin pump that cuts some of the wireless connections between parts of the system. Other researchers are looking for security solutions for pacemakers and cardiac defibrillators. Some researchers have suggested protecting the devices with passwords, but doctors and nurses would have to be able to control the devices in the case of an emergency. "If you have a patient that's unconscious on the ground, you really don't want the medical staff to have to figure out what security system they're using," said University of Washington's T. Denning at the recent CHI 2010 conference. The passwords could be tattooed in the form of a barcode on the patient's skin, either with visible ink or ink that can only be seen under ultraviolet light, Denning said. Security issues for medical devices will increase when these devices are connected to phones, the Internet, and other computers, notes University of Massachusetts at Amherst professor K. Fu.

## Researcher Aims to Secure RFID Tags
**IDG News Service (04/16/10), N. Barber**

Technology for providing alerts when information on radio-frequency identification (RFID) tags is being accessed and controlling access to private information was on display during the recent CHI 2010 conference. Working with Microsoft Research, N. Marquardt, a Ph.D. student at the University of Calgary, has developed four prototype RFID controller groups. The first group provides direct feedback to users by either lighting up, vibrating, or making a sound when the tag is being accessed. The next group features controllable tags, including a button that has to be pressed to activate the RFID and a touch sensitive tag that has to be held to read its information. In the third group, one tag is light sensitive and prevents data from being accessed when the RFID card is in a pocket, and the other tag is tilt sensitive and can only be accessed when pressed flat against a reader. The fourth group makes some information on an RFID tag always accessible, but more private information can only be accessed by moving the tag closer to the reader.

## Keeping Medical Data Private
**Technology Review (04/13/10), K. Gammon**

Vanderbilt University (VU) researchers have developed an algorithm designed to protect the privacy of medical patients while maintaining researchers' ability to analyze large amounts of genetic and clinical data. Although patient records are anonymized, they still contain the numerical codes, known as ICD codes, which represent every condition a doctor has detected. As a result, VU professor B. Malin says it is possible to follow a specific set of codes backward and identify a person. Malin and his colleagues found that they could identify more than 96% of a group of patients based only on their particular set of ICD codes. To make patients more private, the researchers designed an algorithm that searches a database for combinations of ICD codes that distinguish a patient and then substitutes a more general version of the codes to ensure each patient's altered record is indistinguishable from a certain number of other patients. The researchers tested the algorithm on 2,762 patients and could not identify any of them based on their new ICD codes.

**Cyberattack on Google Said to Hit Password System**
**New York Times (04/19/10), J. Markoff**

The cyberattack against Google's computer networks, first disclosed in January, also reportedly breached the company's password system, called Gaia, which controls user access to almost all of its Web services. Although the hackers do not appear to have stolen the passwords of Gmail users, the Gaia breach leaves open the possibility that hackers may find other unknown security weaknesses. The intruders were able to gain control of a software depository used by the Google development team by luring an employee to a poisoned Web site through a link in an instant message. "If you can get to the software repository where the bugs are housed before they are patched, that's the pot of gold at the end of the rainbow," says McAfee's G. Kurtz. An attacker looking for weaknesses in the system could benefit from understanding the algorithms on which the software is based, says Neustar's R. Joffe. Google still uses the Gaia system, although now it is called Google Sign-On. Soon after the intrusion, Google activated a new layer of encryption for its Gmail service. The company also tightened the security of its data centers and further secured the communications links between its services and the computers of its users.

**Secure P2P Scheme Leverages Social Networks**
**InformationWeek (04/19/10), T. Claburn**

Microsoft and Catholic University of Leuven researchers are proposing Drac, a method to secure anonymous instant messaging (IM) and voice-over-IP (VoIP) communication using peer-to-peer technology. Drac makes IM and VoIP traffic anonymous and unobservable by exposing the social connections of the users who make up the nodes of the peer-to-peer network. "Drac gives away the identity of a user's friends to guarantee the unobservability of actual calls, while still providing anonymity when talking to trusted third parties," the researchers say. Although anonymous online communications may conceal the content of conversations, information about the network addressing the timing of messages and the volume of traffic often reveal as much as the hidden correspondence, according to the researchers. Drac is designed to preserve anonymity while also stopping traffic analysis by using a peer-to-peer relay architecture that routes data through social networking connections.

**Pentagon Turns to 'Softer' Sciences**
**Nature (04/14/10), S. Weinberger**

The US Defense Department's defense research and engineering office is overseeing a budget migration away from applied research and into disciplines such as biology, computer science, the social sciences, and cybersecurity. Defense chief technology officer Z. Lemnios says that cybersecurity is a priority for Defense Department researchers, and last summer he launched a joint study with the Intelligence Advanced Research Projects Activity to examine the best areas where cybersecurity funds should be committed. The results of the study are being fed into a proposal to Congress for a new $200 million cybersecurity research and technology program. Lemnios told a House of Representatives panel that his office will underwrite research to "harden key network components; increase the military's ability to fight and survive during cyberattacks; disrupt nation-state level attack planning and execution; measure the state of cybersecurity; and explore and exploit new ideals in cyberwarfare".

### Random, But Not By Accident: Quantum Mechanics and Data Encryption
### UM Newsdesk (04/13/10), L. Tune

Researchers at the University of Maryland's Joint Quantum Institute (JQI), working with European quantum information scientists, have demonstrated a method of producing certifiably random strings of numbers based on the fundamental principles of quantum mechanics. The technique is based on the work of physicist J. Bell, who studied a condition called entanglement, in which matter particles become so interdependent that if a measurement is performed to determine a property of one, which will be a random value, the corresponding property of the other is instantly determined as well. Bell showed mathematically that if the objects were not entangled, their correlations would have to be smaller than a certain value, expressed as an "inequality." However, if they were entangled, their correlations could be higher, violating the inequality. The JQI test was the first to violate a Bell inequality between systems separated over a distance without missing any of the events. "If we verify a Bell inequality violation between isolated systems while not missing events, we can ensure that our device produces private randomness," says JQI's D. Matsukevich.

### Quantum Cryptography Hits the Fast Lane
### ScienceNOW (04/19/10), A. Cho

Toshiba researchers have developed a quantum cryptography system they say is fast enough to encrypt a video transmission. The system can send bits of key at a megabit per second across a 50-kilometer fiber, says Toshiba's A. Shields. The researchers also have demonstrated that the system can run continuously for 36 hours. The key to running faster is a better photon detector, Shields says. The Toshiba system use devices called semiconductor avalanche photodiodes, in which a photon hits a bit piece of semiconductor to trigger an "avalanche" of electric charge. New photodioes can detect smaller avalanches and run faster, according to Shields. The researchers used a feedback system to stretch certain optical fibers by a few nanometers, which keeps the ratio of those lengths constant and enables the system to run for hours at a time. Without such stabilization, key distribution would have to stop every few minutes to allow the equipment to recalibrate itself.

### Spammers Pay Others to Answer Security Tests
### New York Times (04/25/10), V. Bajaj

Spammers are paying people in countries such as India, Bangladesh, and China to pass Web security tests known as CAPTCHAS, which ask Web users to type in a string of semi-distorted characters to prove they are humans and not spam-generating robots, according to Carnegie Mellon University professor L. von Ahn. He says thousands of people in developing countries, primarily in Asia, are solving these puzzles for pay. The completed CAPTCHAS help spammers open new online accounts to send junk emails. However, Internet company executives say the threat of spammers paying people to decode CAPTCHAS is not a major concern. They note that Web sites use several tools to verify accounts and maintain security. Some sites may send confirmation codes as text messages, which then must be entered into a separate verification page before new email accounts are activated. "Our goal is to make mass account creation less attractive to spammers, and the fact that spammers have to pay people to solve CAPTCHAS proves that the tool is working," says Google's M. Hughes.

### Tracking Criminal Data Centers
### Technology Review (04/23/10), E. Naone

Malicious content on the Web can be very difficult to stop, said security experts at the recent Source Boston computer security conference. The difficulties involved in stopping malicious Web content can be seen in the 2008 shutdown of the malicious hosting company McColo, which at one point was responsible for more than 66% of the spam on the Internet. Although that spam stopped when McColo was shut down, botnets, such as the Grum, have taken its place, according to FireEye security researcher A. Lanstein. He says that he has tried and failed to shut down SteepHost, the Ukraine-based company that is hosting the block of IP addresses that Grum uses for its attacks. But even if malicious hosting companies such as SteepHost were shut down, another company would quickly replace it, Lanstein says. An additional obstacle involved in stopping malicious Web content is the fact that IP addresses cannot be confiscated as long as their owners have paid for them, Lanstein says. Rapid chief security officer HD Moore says that it will continue to be difficult to shut down malicious hosting companies after IPv6 is introduced, since the implementation of the protocol would enable companies to purchase large blocks of IP addresses in order to evade tracking.

### NSA's Boot Camp for Cyberdefense
### CNet (04/22/10), D. Terdiman

The US National Security Agency (NSA) has been conducting its 10th annual Cyber Defense Exercise, a contest that pits students from various military academies against each other and against the competition's leaders at NSA in a bid to see whose cyberdefense skills are superior. The objective is to help the students learn about information assurance and its application toward the protection of the most crucial information systems in the United States and Canada. Air Force Capt. M. Henson says the participants are tasked with building a network with all of the services mandated by the NSA's directive. They must then keep those services operational while battling attempts to bring them down electronically. "All of the faculty have agreed that it is important for the students to be exposed to situations where they can't guarantee a system is 100% locked down and have to react when that system is inevitably compromised," Henson says. He notes that much of the technology and methods that NSA uses against the student teams also is available in the commercial Internet.

### New Research Offers Security for Virtualization, Cloud Computing
### NCSU News (04/27/10), M. Shipman

North Carolina State University (NCSU) researchers have developed HyperSafe, software for resolving security concerns related to data privacy in virtualization and cloud computing. A key threat to virtualization and cloud computing is malicious software that enables computer viruses to spread to the underlying hypervisor, which allows different operating systems to run in isolation from one another, and eventually to the systems of other users. HyperSafe leverages existing hardware features to secure hypervisors against such attacks. "We can guarantee the integrity of the underlying hypervisor by protecting it from being compromised by any malware downloaded by an individual user," says NCSU professor X. Jiang. HyperSafe uses non-bypassable memory lockdown, which blocks the introduction of new code by anyone other than the hypervisor administrator. HyperSafe also uses restricted pointer indexing, which characterizes a hypervisor's normal behavior and prevents any deviation from that profile.