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

**Δελτίο 170**
**15 Μάρτη 2010**

**How to Spot Suspicious VoIP Signals**
**Technology Review (02/25/10)**

Researchers at the Warsaw University of Technology in Poland have studied the characteristics of voice over Internet Protocol (VoIP) calls in an attempt to gain a better understanding of ordinary traffic. Security remains an issue for VoIP calls, which can be hijacked and used to send confidential information over the Internet. W. Mazurczyk and colleagues decided to study ordinary VoIP calls so experts would have a way to compare and contrast regular calls with those that have been embedded with stolen data. VoIP calls can be compromised by changing the order in which the digital packets are sent, or by deliberately delaying certain packets that have embedded data, a technique known as Lost Audio Packet Steganography (LACK). The team's research shows that packets are not normally re-ordered in a way for hiding data, so attacks that re-order data are not a real threat. However, LACK attacks would be difficult to spot because of the routine loss of data packets.

**In Networks We Trust**
**ICT Results (02/24/10)**

European researchers working on the Remote EnTrusting by RUn-time Software authentication (RE-TRUST) project have proposed a solution to trusted computing that they say offers better security and authentication. RE-TRUST uses logic components on an untrusted machine to allow for remote entrusting authentication. "RE-TRUST will have a major impact on all commercial applications and solutions where security or trust is a concern, independently of whether they are based on a client-server or a peer-to-peer paradigm," says RE-TRUST coordinator Y. Ofek. RE-TRUST solutions could work with peer-to-peer networks to enable them to become a new trusted distribution channel. The RE-TRUST team also developed trust solutions for code mobility, reconfigurable computing for software protection, and orthogonal replacement. "All applications and solutions running over a network, such as the Internet, can benefit from the RE-TRUST approach," Ofek says.

**The Safe Way to Use One Internet Password**
**Queensland University of Technology (02/25/10), R. Wilson**

Queensland University of Technology (QUT) Ph.D. researcher Suriadi is investigating using an anonymous credential system, an Internet authentication system from the 1980s, to enable Web users to securely log in only once per Internet session. Suriadi says future single sign-on systems could give users access to multiple accounts--including email, bank, and shopping--but would need to provide extreme privacy to avoid hackers. He says the anonymous credential system could enhance the security and privacy of a single sign-on system. "The system works by revealing as little information about who you are as necessary for logging into an account, therefore allowing you to remain anonymous," Suriadi says. A single sign-on system backed by the anonymous credential system requires the cooperation of business and organizations to enable it, Suriadi notes.

**GPS Vulnerable to Hacker Attacks**
**BBC News (02/23/10), J. Palmer**

Experts warn that technology reliant on satellite navigation signals is increasingly vulnerable to attack from widely available equipment. At a UK conference at the National Physical Laboratory, professor D. Last said the global positioning system's (GPS's) biggest vulnerability is the extreme weakness of the signals that reach receivers, which allows jamming by Earth-based equipment to be executed. Such jamming has been conducted by military systems for years to disrupt adversaries' navigation systems, but small jamming devices are increasingly available online. Moreover, receivers can be fooled into accepting erroneous data by bogus GPS signals, Last warned. Seagoing vessels are especially susceptible to GPS hacking, given that their systems increasingly use satellite navigation directly as well as feed GPS signals into other equipment.

**US Plan to Make Hacking Harder Revealed**
**Financial Times (03/03/10) P. 4; J. Menn**

The Obama administration has declassified part of its plan to improve the security of cyberspace in an attempt to cultivate greater collaboration between government and civilian groups. More cooperation between the private sector and the US National Security Agency is the centerpiece of the Comprehensive National Cybersecurity Initiative (CNCI). The declassified abstract of the plan reveals that the US Dept. of Homeland Security will operate a new security system, called Einstein 3, that analyzes email and other data traffic into and out of federal networks. CNCI also urges merged oversight of federal spending on research and development in cybersecurity, with a particular focus on "leap-ahead" technology. Although the initiative acknowledges that traditional security approaches "have not achieved the level of security needed," it says the federal government is now outlining "grand challenges" for the research community to help solve the most difficult problems.

**Software Sniffs Out Criminals By the Shape of Their Nose**
**University of Bath (03/02/10), V. Just**

University of Bath scientists have developed a biometric system for identifying people based on their nose shape. The researchers used a photographic system called PhotoFace to scan the three-dimensional shape of volunteers' noses and used software to analyze them according to six main nose shapes. The researchers focused on the ridge profile, the nose tip, and the section between the eyes at the top of the nose. The researchers say their system offers a good recognition rate and a faster rate of image processing than whole face recognition techniques. "The technique is able to achieve a level of detail that is beyond current competing technologies and can be extended to a myriad of other applications, ranging from industrial surface inspection to cosmetics," says University of West England professor M. Smith. The researchers plan to build a larger database of noses to test the software to see if it can identify individuals from a bigger group of people or from blood relatives.

**Researchers Find Weakness in Common Digital Security System**
**University of Michigan News Service (03/03/10), N. C. Moore**

University of Michigan (UM) researchers have found weaknesses in the RSA authentication encryption method, which is used to protect both media copyright and Internet communications. The scientists discovered they could breach the system by varying the voltage supply to

the holder of the "private key," which would be the consumer's device in the case of copy protection and the retailer or bank in the case of Internet communications. Private keys contain more than 1,000 digits of binary code and would take longer than the age of the universe to guess, says UM doctoral student A. Pellegrini. However, using the voltage disrupting method, the UM researchers were able to obtain the private key in about 100 hours. Changing the electric current confuses the computer and causes it to make small mistakes in its communications with other clients. These faults reveal small pieces of the private key. After enough faults were created, the researchers were able to reconstruct the key offline without damaging the device.

**Feds Weigh Expansion of Internet Monitoring**
**CNet (03/04/10), D. McCullagh**

A future expansion of Internet communications monitoring to the private sector is being considered by the US Dept. of Homeland Security (DHS) and the National Security Agency. DHS cybersecurity official G. Schaffer says the department is assessing whether its Einstein 3 system for detecting and preventing cyberattacks "makes sense for expansion to critical infrastructure spaces" over time. Although some civil-liberties advocates warn the technology could be used to snoop on private networks, Schaffer dismisses such notions. "As a practical matter, you're looking at data that's relevant to malicious activity, and that's the data that you're focused on," he says. However, Tor anonymity project programmer J. Appelbaum says that expanding Einstein 3 to private companies would be tantamount to partly outsourcing security, and warns that "anyone with access to that monitoring system, legitimate or otherwise, would be able to monitor amazing amounts of traffic."

**The Next Secure Hash Algorithm Had Better Be a Good One**
**Government Computer News (03/03/10), W. Jackson**

The National Institute of Standards and Technology is in the middle of a multi-year competition to pick the next hash algorithm, to be called SHA-3, which will be used to protect government files. Katholieke Universiteit Leuven professor B. Preneel says SHA-3 will need to be sophisticated enough to withstand hacker attempts for the next 20 years. "It is unlikely there will be another competition (for SHA-4) before 2030," Preneel says. However, some observers say the selection process is moving too quickly. "I think they should pick three winners, not one, and spend several years studying them," says former National Security Agency technology director B. Snow. The contest started with 51 algorithms, which were narrowed down to 14 in the first round. Researchers are now examining the 14 algorithms and are expected to pick a final 5 in late 2010. Both Snow and Preneel are concerned that not enough time is being given to thoroughly vet the remaining algorithms before a final choice is made.

**NC State Research Advances Voice Security Technology**
**North Carolina State University (03/08/10), M. Shipman**

A North Carolina State University (NCSU) research team led by professor R. Rodman has developed a computer model that accelerates the voice identification process without sacrificing accuracy. Existing computer models take several seconds or longer to compare acoustic profiles and identify a speaker, which is too long for the technology to be widely used, according to Rodman. "In order for this technology to gain traction among users, the response time needs to improve without increasing the error rate," he says. The researchers modified exist-

ing computer models to make the authentication process work more efficiently. "This is part of the evolution of speech authentication software, and it moves us closer to making this technology a practical, secure tool," Rodman says.