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

**Δελτίο 167**
**30 Γενάρη 2010**

**Cryptographic Showdown, Round 2: NIST Picks 14 Hash Algorithms**
**Government Computer News (01/05/10), W. Jackson**

The US National Institute of Standards and Technology (NIST) has completed round one of its open competition to create a new Secure Hash Algorithm (SHA). The cryptographic community narrowed the first round's 64 submissions down to 14 semifinalists. Fifty-one of the 64 algorithms submitted in 2008 met the competition's minimum criteria, and it took the judges a year to examine the entries for flaws and weaknesses. "We were pleased by the amount and quality of the cryptanalysis we received on the first round candidates, and more than a little amazed by the ingenuity of some of the attacks," says NIST's B. Burr. Five finalists are expected to be named from the 14 remaining entries by the end of this year, and a new standard, which will be named SHA-3, should be ready in 2012. SHA-3 will replace the SHA-1 and SHA-2 algorithms currently being used by NIST. This is the third open cryptographic competition conducted by NIST, the first coming in the 1970s, and the second in the 1990s.

**Google Threatens to Leave China After Attacks on Activists' E-mail**
**Washington Post (01/13/10) P. A1; E. Nakashima, S. Mufson, J.Pomfret, et al.**

Google has threatened to withdraw from China following a computer network attack targeting its email service and corporate infrastructure. Google claimed to have proof suggesting that "a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists," while noting that at least 20 other large firms have been targeted by similar attacks. US officials have avoided leveling a public charge against China for the attacks because it is difficult to determine the assault's origins with certainty. Google chief legal officer D. Drummond says the hacks drove the company to "review the feasibility" of its Chinese operations, while realizing that this could entail the shutdown of Google.cn and Google's China offices. He also says that Google has elected to halt its censoring of search results on Chinese Google sites, and over the next few weeks the company will engage in discussions with China on the possibility of running "an unfiltered search engine within the law, if at all." Center for Democracy and Technology president L. Harris lauds Google's move, saying the company "has taken a bold and difficult step for Internet freedom in support of fundamental human rights."

**Fixing a Hole in the Web**
**Technology Review (01/12/10), E. Naone**

A fix that the Internet Engineering Task Force recently approved to patch a vulnerability in the protocol that encrypts sensitive Web-based communications and transactions is expected by experts to take a year or more to be fully deployed. The patch fixes the Transport Layer Security (TLS) protocol, which is built into Web browsers and servers and shields critical information, and which has supplanted the Secure Socket Layer protocol. By exploiting the TLS flaw, an attacker can commandeer the first moment of the encrypted conversation between a Web browser and server and insert a command of his own. Exploiting the vulnerability requires the hacker to first carry out a man in the middle attack to capture traffic between

the client and the server, and then take advantage of TLS' renegotiation feature. This feature permits a Web server or client to revise some of the parameters of an encrypted session while the session is taking place. Security professional F. Breedijk says the protocol is patched by a draft fix that effectively produces two versions of TLS--thus keeping the danger of attack alive if either the client or the server fails to install the patch. Apache Software Foundation founding director B. Laurie says that this double installation requirement makes the fix "unprecedented," so browser makers working to correct the problem will need to make accommodations for a period in which the client will continue communicating with unpatched servers.

**Companies Fight Endless War Against Computer Attacks**
**New York Times (01/17/10), S. Lohr**

The growing sophistication of cyberattackers and the susceptibility of even the best defensive measures are highlighted by the recent attacks against Google from within China, according to security experts. Despite the billions of dollars that government agencies and corporations are spending each year on specialized anti-malware programs, malicious hackers appear to have the edge. A recent Computer Security Institute (CSI) survey of nearly 450 companies and government agencies found that 64 percent reported malware infiltration, versus 50% the previous year. CSI director Robert Richardson says that malware is an ever-growing threat, and notes that "now the game is much more about getting a foothold in the network, for spying." Some experts say the long-term solution to the threat of malevolent hackers is to steer the software industry on a path toward maturation, with standards, defined responsibilities, and accountability for security lapses directed by forceful self-regulation or by the government.

**Today's Threat: Computer Network Terrorism**
**University of Haifa (01/17/10)**

The University of Haifa's Y. Levyatan says that cyberterrorism is just as much of a threat to today's governments as more conventional forms of terrorism. "A fleet of fighter planes is not necessary to attack a power station; a keyboard is sufficient," Levyatan says. "And if you don’t have the skills, there are enough mercenary hackers who can do it for you." Among international hackers, there is a growing trend to threaten national infrastructures for ransom, he says. Recently, most online fighting has focused on attempts to immobilize leading Web sites, but the next step is to target systems controlled by computer networks such as financial systems, power stations, hospitals, television broadcasts, and satellites, Levyatan says.

**Hillary Clinton Calls for Web Freedom, Demands China Investigate Google Attack**
**Washington Post (01/22/10), C. Kang**

In a sweeping Internet freedom speech, US Secretary of State H. Clinton called for a global Internet free of censorship in response to claims that hackers targeted Chinese human rights activists' Google accounts. The US State Department has sent a formal request to the Chinese government asking for a review of the claims. Clinton also called for all nations to work together to punish cyberattacks aimed at silencing citizens and disrupting businesses. "Countries or individuals that engage in cyberattacks should face consequences and international condemnation," Clinton says. The rise in social networking has led some countries such as Iran, Uzbekistan, Vietnam, and Tunisia, to try to block online traffic. The United States will push to preserve the ability of everyone to communicate freely over the Web, Clinton says.

The State Department also plans to work with non-government organizations and technology companies on solutions to the problem of Internet censorship abroad.

**Clarkson University Professor's Software to Test Cybersecurity Systems for Flaws**
**Clarkson University News (01/25/10), M. Griffin**

Clarkson University (CU) scientists, in collaboration with researchers from the University at Albany-SUNY, the University of New Mexico, the University of Illinois, and the Naval Research Laboratory are developing software that will test cybersecurity systems for flaws. CU professor C. Lynch wants to use automated reasoning to teach machines to scan cybersecurity systems for glitches. The research effort's goal is to design a program that can find cybersecurity flaws in a system before it hits the commercial market. "When you work in cybersecurity, everything has to be just right," Lynch says. "One little thing might be off, and that's the hole the intruder needs to come through and get everything." He says the system could have applications in a wide variety of fields, from banking to national security. "It would deal with pretty much anything where you need to be sure your information is kept secret," Lynch says. "The point is that almost everything in our lives today involves computers. We need them to be secure."

**Survey of Executives Finds a Growing Fear of Cyberattacks**
**New York Times (01/28/10), J. Markoff**

Cyberattacks are a growing threat to the critical infrastructure underlining modern society, according to a survey of 600 computing and computer-security executives in 14 nations conducted by McAfee and the Center for Strategic and International Studies. Study director S. Baker cites findings that 50% of respondents believe they have already been the target of sophisticated government hackers. More than half of the polled executives say that their own country's laws do not adequately discourage cyberattacks, and the three most vulnerable nations are identified as the United States, China and Russia. 40% of executives are anticipating a major cybersecurity incident in their sector within the next year, while all but 20% project such an incident occurring within five years. The report indicates that the growing use of Internet-based networks "creates unique and troubling vulnerabilities," although the authors stop short of urging a complete partitioning of systems and the open Internet. "Remote access to control systems poses a huge danger," warns McAfee's P. Schneck.

**Researchers Criticize 3D Secure Credit Card Authentication**
**Heise Online (United Kingdom) (01/26/10)**

University of Cambridge Computer Laboratory researchers S. Murdoch and R. Anderson contend in a paper that the 3D Secure (3DS) credit card authentication system branded as the MasterCard SecureCode and Verified by Visa schemes is deeply flawed. The researchers call attention to a number of vulnerabilities. For instance, the mechanism used to display the 3DS form is incorporated within an iframe or pop-up with no address bar, leaving no clue as to the form's origin. This conflicts with banks' recommendation to customers to avoid phishing sites by only entering bank passwords into sites they can identify as the bank's own site. The initial password entry process that takes place the first time a cardholder uses a 3DS-enabled card to shop online also is a point of criticism, as the user is asked to enter a new password as part of the process of facilitating the purchase. Murdoch and Anderson argue that the timing of this request is wrong, as the shopper is probably more interested in the transaction than security and is more likely to select a weak password. The paper cites the single sign-on model

that the 3DS system deploys as inappropriate, and says that it should be supplanted by a transaction authentication system in which a user receives a SMS message asking for an authorization code from the shopper.

**e-Passports Threaten Your Privacy**
**University of Birmingham (01/19/10), K. Chapple**

University of Birmingham (UB) researchers have discovered a flaw in e-passports that makes them susceptible to identification. The defect is in the design of the radio-frequency identification tag used by e-passports. The discovery makes it possible to detect the passport of a particular person from a distance of a few meters. An attacker can track the movements of a specific passport by replaying a particular message. "Our discovery has shown that there is a flaw that makes it possible to identify the movements of a particular passport without having break the passport's cryptographic key," says UB researcher T. Chothia. e-passports have been issued to more than 30 million people.