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

Δελτίο 143
15 Μάρτη 2009

Computer Scientists Deploy First Practical Web-Based Secure, Verifiable Voting System, Harvard University (03/05/09), M. Rutter

The Harvard School of Engineering and Applied Sciences' Center for Research on Computation and Society (CRCS) and scientists at the University Catholique de Louvain in Belgium deployed a Web-based, secure, verifiable-voting system for the Belgium presidential election that was held in early March. Called Helios, the system was developed by CRCS fellow B. Adida. "Helios allows any participant to verify that their ballot was correctly captured, and any observer to verify that all captured ballots were correctly tallied," Adida says. "We call this open-audit voting because the complete auditing process is now available to any observer." The open source software uses advanced cryptographic techniques to maintain ballot secrecy while providing a mathematical proof that the election tally was correctly computed. Helios uses public-key homomorphic encryption, a method in which a public key is used to encrypt a message, or a vote. Homomorphic encryption allows messages to be combined while still encrypted, which works for counting votes, and requires multiple private keys to decrypt a message, which was the election tally. In an election, voters receive a tracking number for each of their votes, and each vote is encrypted with the election public key before leaving the voter's browser. Voters can then use their tracking numbers to verify that their ballot was correctly captured by the voting system, which publishes a list of all tracking numbers received before tallying. Finally, the voter, or any observer, can verify that the tracking numbers and votes were tallied appropriately. Adida says the encryption allows the entire verification process to take place without revealing the contents of each vote.

Fight Over Internet Filtering Has a Test Run in Europe
New York Times (03/09/09) P. B7; K. O'Brien

Europe's influence over technology regulation has led US companies to send lobbyists to try and influence European lawmakers as they debate Internet access policy. "The US companies see the outcome of the fight in Europe as key," says J. Zimmermann, a lobbyist for French Internet advocacy group La Quadrature du Net. "Each side is hoping to score points on the issue here so they can take it back to the [US] to influence the outcome there." Net neutrality is supported by free-speech advocates and Internet businesses that want to prevent network operators from filtering Internet traffic, but Internet service providers say that basic traffic management is needed to deal with the soaring demand for bandwidth. The outcome of the debate over net neutrality could affect whether consumers will continue to have access to unlimited bandwidth for downloads on a flat-rate plan, or if they will have to pay higher fees based on the amount of data they download. European lawmakers are split on the issue, and much of the debate is taking place in Belgium, where lawmakers are close to making a decision and two committees are expected to vote on March 31 before the issue goes before Parliament on April 22. With more than 200 network operators in Europe, as opposed to the five major broadband and four cable operators in the US, the danger that one operator could filter Internet traffic for commercial gain is rather low, says Liberty Global's M. Kohnstamm.

A Struggle Over US Cybersecurity
Washington Post (03/10/09) P. A11; B. Krebs

R. Beckstrom, the US federal government's cybersecurity coordinator, has resigned after less than a year on the job, citing a lack of funding and the National Security Agency's (NSA's) growing control over government cybersecurity measures. Beckstrom was director of the National Cyber Security Center, which was launched last March to help coordinate cybersecurity efforts between intelligence communities. However, he says recently there have been efforts to fold the National Cyber Security Center into the NSA. Beckstrom says the center was created to coordinate the various agencies' efforts and not to be controlled by NSA. "This is a coordination body and it resides alongside or above the other centers, but certainly not below them," he says. "In my view, it is very important that there be independence for the [center], and that it be able to carry out its role." The Obama administration is currently in the middle of a 60-day review of the government's cybersecurity initiative, and is expected to release recommendations sometime next month. Last month, director of national intelligence Adm. D. Blair told the House Intelligence Committee that NSA was the proper agency to preside over protecting military and government networks. The National Cyber Security Center was part of the Bush administration's comprehensive national cybersecurity initiative to protect the government against online attacks.