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

**Δελτίο 84**
**23 Ιουλίου 2007**

### Re-Vote Likely After E-Vote Error
### IDG News Service (07/14/07), S. Lawson

A Berkeley, Calif., city initiative is likely to be put back on a ballot because of the mishandling of electronic voting machine data. Judge Winifred Smith of the Alameda Country Superior Court indicated that she would nullify the defeat of the medical marijuana initiative in Berkley in 2004 and order the measure to be put on a ballot in a later election. The case highlights the dangers of electronic voting, which makes it harder to ensure fair elections, says attorney Gregory Luke, who is representing Americans for Safe Access, a medical-marijuana advocacy group that is suing the county. Americans for Free Access wanted a recount of the vote for Measure R in 2000, which would have established procedures for opening marijuana dispensaries in Berkeley, and was defeated by fewer than 200 votes. A recount was not possible because the city failed to share necessary voting records, a violation of election laws, Judge Smith ruled in April. Luke says the country reused voting machines from Diebold election Systems without saving enough data to have a recount or to review the election. Additionally, election officials failed to save key evidence after the suit was pending, and data from the vote in question has been found on only 20 out of the hundreds of machines used in the election, Luke argued.

### Three Hamilton Students Examining Computer Security for Summer Research Project
### Hamilton College (07/12/07)

The Air Force Research Lab in Rome, N.Y., is sponsoring the computer security-related summer projects of three students from Hamilton College. One project will focus on how the formal access policies of SE-Linux are defined, and how they are enforced by the Dept. of Defense-sponsored secure operating system that controls computer use. Student K. Gorman will write new programs to help determine failure in the policies, and show how policies can be written to improve the security of operations. Meanwhile, students C. Prime and T. Williams will team up to define a framework for "live" computer forensics. Prime will concentrate on rootkits and Williams will focus on other kinds of malware, with the goal of creating a new framework for recognizing such programs while machines are still running and possibly under attack. Professor S. Hirshfield is overseeing the computer security research efforts of the students.

### Computer Science Prof Researches Program Safety
### Regina Leader-Post (CAN) (07/10/07), J. Couture

Philip Fong, a computer science professor at the University of Regina, views the granting of access rights only to programs on a need-to-know basis as a way to make computers safer. He uses the game Solitaire as an example of a program that has all the access rights of computer users, and is not considered to be dangerous. "But as soon as vulnerabilities of these seemingly safe programs get discovered by malicious parties, they could exploit them to attack our machines," he says. Thanks to nearly $250,000 in funding from the National Sciences and Engineering Research Council of Canada (NSERC), Fong plans to create a software language that is trustworthy and a deployment platform for safely running untrusted software. "My research really is about how to build programming abstractions or programming languages that would allow us to implement the principle of granting only enough access rights to a program so that they can function, rather than granting them all the rights that we have as users," he says. Fong wants to develop open source tools that software developers can build on and use to create safe applications.

### Cyberterrorism: By Whatever Name, It's on the Increase
### InformationWeek (07/09/07)No. 1145, P. 32; L. Greenemeier

Recent incidents in Russia and England suggest that criminals are increasingly using the Web to organize or initiate Web attacks intended for political or cultural treason. In Britain, three Muslim men dubbed "cyber-jihadis" were convicted of inciting Muslims to attack non-Muslims via the Internet; the men received prison terms of up to 10 years. The US Computer Emergency Readiness Team described Russian cyberattacks that struck political Web sites such as the United Civil Front. Moreover, cyberwarfare has existed for months, with a Russian newspaper, a Russian radio station, and Estonia's cyberinfrastructure all targeted by denial-of-service attacks in April 2007 and May 2007. On the jihadi Web site Al-jinan.org, the "Electronic Jihad Program" is an application that lets users select a Web site to attack. Al-jinan has existed for over four years, but contradictions in its domain name server registration make it hard to track its source. Large-scale cyberattacks would significantly affect American businesses, as companies in the private sector run most of the country's crucial infrastructure. Still, everyone must be aware of security issues, as electronic jihad is out to produce economic disruption of any kind.

### Mounting Scrutiny for Google Security
### InfoWorld (07/12/07)

Search behemoth Google is experiencing an increasing amount of examination as it expands into the business sector with new products. Ponemon Institute researchers have completed a report focusing on the only substantial security flaw found in the Google Desktop program, to date; the flaw was a cross site scripting vulnerability discovered and patched in February 2007 by Google. Still, the Ponemon report reveals that nearly three quarters of the approximately 600 IT security specialists polled believe that Google Desktop probably contains other security flaws. Google recently acquired GreenBorder Technologies and Postini to augment its security skills and sponsored Stopbadware.org, a malware research project. However, Ponemon contends that Google's prominence in the market makes it an increasinggly attractive target to hackers. Google's intent to cultivate "deep integration" between Web-based and desktop tools has also concerned some who believe that remote queries can jeopardize sensitive data stored on computers. Google CIO D. Merrill says Google pays more than 1,000 engineers to test for gaps in its software, encourages communication between technology providers, security researchers, and white hat hackers, and promotes responsible problem disclosure. Google also has an advantage in that problems can be resolved immediately on its servers, unlike companies that must convey patches to all users, notes Merrill. In addition, Google Desktop and Google Apps systems actually add an additional layer of security to joint business endeavors by requiring authentication and by helping companies locate improperly used data. The company also notifies customers of its security efforts and stays informed of cutting-edge attack strategies through Stopbadware.org and the Google Security Blog. Industry experts concur that Google has excelled at safeguarding its users from attacks and major vulnerabilities thus far, but nevertheless recommend that Google learn from Microsoft's mistakes in order to maintain a strong reputation.

**Dan Wallach: Security Watchdog for the Industry**
**Computerworld (07/09/07) Vol. 41, No. 28, P. 58; S. Collett**

D. Wallach is on sabbatical from Rice University, where he is a tenured associate professor, but he continues to focus on making sure key technologies affecting the public are secure. The security researcher is serving as associate director of ACCURATE, and is concentrating on voting security at the $7.5 million research center. Among the many papers that Wallach has published is one that analyzed the Secure Digital Music Initiative and found that all of the proposed systems were very vulnerable. For another research project, Wallach led a team that identified similar security flaws in the electronic voting systems from Diebold. Exposing the security flaws prompted threats of lawsuits from the SDMI consortium and Diebold, but they ultimately decided against mounting a legal challenge to Wallach, who says his claims are backed by scientific evidence. "I'm not a hacker," says Wallach, 35, who even uncovered security flaws in Sun Microsystems' Java technology while pursuing graduate studies at Princeton University. Wallach, who was named one of Computerworld's 40 leading innovators under the age of 40, says he joined ACCURATE because "it's hard for me to think of anything more important [to work on] than our democracy."

**Latest Weapon Against Spam Also Enlists Computer Users to Assist the Internet Archive, Pittsburgh Post-Gazette (07/18/07), L. Yao**

As a graduate student at Carnegie Mellon University in 2000, L. von Ahn worked on Completely Automated Public Turing test to tell Computers and Humans Apart (Captcha), the online tests that ask users to decipher a distorted word to gain access to a site. At first, Captchas were unreadable to computers, but resourceful hackers found ways for computers to solve Captchas. Von Ahn, now an assistant professor of computer science at Carnegie Mellon, then started working on another test. "It's an arms race," von Ahn says. "We come up with something that programs shouldn't be able to read. Then somebody comes up with a way to read it, so we have to come up with a better one." The solution von Ahn released in late may, called reCaptcha, not only provides a secure test, one that von Ahn predicts will take years to break, but also contributes to the Internet Archive, a nonprofit that is working to create digital records of books. The archive project scans books and uses word recognition software, much like hackers do, to create digital records. The problem is that the software is often unable to recognize some of the words in older books. ReCaptcha presents users with two words to decipher, one the archive already knows and one that it was unable to recognize. When enough users have entered the same answer for the unknown word, the archives accepts the stores the word. "We only take words the computer can't read," von Ahn says. "That extra step makes it much more secure, because we just threw away everything a computer could read." Meanwhile, von Ahn is also developing online games that use human intelligence to solve problems computers have problems with. One program, Matchin', asks users to identify attractiveness, allowing an image to be archived and searched for on its degree of "prettiness."

**New Public Surveillance Research**
**Scenta (07/12/07)**

The effectiveness of public surveillance tools and strategies for security and marketing purposes is the subject of two separate research projects of students from the University of Southampton's School of Electronics & Computer Science. In "A Comparison of Background Subtraction Techniques," S. Deene notes that background information often prevents the display of a clear image of an object in closed-circuit television (CCTV) footage, then combines a number of current methods to develop her own system. "It was apparent that a simple subtraction algorithm was needed to allow the high computational efficiency that is required by CCTV applications," says Deene, in highlighting the complexity of background subtraction. Meanwhile, Matthew Sharifi examined how well face recognition software and Bluetooth recognize faces in "Audience Recognition in Public Spaces." All of the frontal faces seen in a reception area were picked up by a camera but only 8.33% by Bluetooth, in which individuals also needed to carry the devices, and the results of the study has Sharifi considering pursuing a larger video dataset so he can continue the research. Sharifi says "it would be interesting to combine the two techniques into a multi-modal identification technology which could couple the ubiquity of face recognition with the recognition accuracy of Bluetooth."

### Old Flaw Threatens Web 2.0
### Dark Reading (07/12/07), K.-J. Higgins

A browser technology that is designed to prevent malicious servers from hijacking HTTP sessions has a vulnerability that poses a threat to Internet users and corporate intranets. The technology, called DNS pinning, is vulnerable because it attempts to bind a single IP address to a single domain name. However, this does not work because there are a number of things that can run inside a browser that do their own DNS lookups, including XML and Java plug-ins. This vulnerability can be exploited in a number of ways. For instance, attackers can lure a victim to a malicious Web site, which can be used to establish a VPN connection straight to the victim's corporate network. There is currently no way to patch this vulnerability. But organizations can still take several steps to address this problem, including adding stronger authentication for internal, Web-based sensitive content, using the same level of security testing and "hardening" as for public Web applications, and using SSL for accessing internal applications, according to a white paper written by NGS Software principal security consultant D. Stuttered. Meanwhile, security researchers are investigating how to mitigate the DNS pinning flaw. "There is a lot more research to be done in this area," says WhiteHat Security founder J. Grossman. "It's not going to stop anytime soon."

### Salary Premiums for Security Certifications Increasing, Study Shows
### Computerworld (07/09/07), J. Vijayan

Recent statistics show that a professional security certification will enable information technology security workers to earn higher salaries. For example, a Foote Partners study released the first week of July concludes that security professionals with security certifications earn up to 15% more than their non-certified colleagues. And from October to April, a group of 27 security certifications examined by the Foote study grew in value by an average of 1.7 %. Foote Partners CEO D. Foote says that demand for certified security professionals is growing following a recent downturn. And the demand is being driven not by compliance and government regulation, but by customers who are "demanding more security" from companies. The fallout from major data breaches such as the TJX breach has caused consternation among corporate executives, prompting many executives to make additional commitments to security. A Dept. of Defense mandate requiring certification from IT security professionals is also increasing demand for certified security professionals, says Foote.

## Professor Denning Tapped by NSF
## Naval Postgraduate School (07/13/07), B. Honegger

Naval Postgraduate School Dept. of Computer Science chairman P. Denning has been named one of two winners of the first ever National Science Foundation Computer and Information Science and Engineering (CISE) Distinguished Education fellowships. As such, he will receive a two-year $250,000 grant to improve the quality of computer science education in undergraduate schools under the NSF's Pathways to Revitalized Undergraduate Computing Education program. "We need to inspire the best and the brightest to go into computing," said CISE Assistant Director J. Wing in presenting the award. "The United States is the world leader in computer science and engineering, but other nations are quickly catching up as enrollment in traditional US computer science programs is declining. These fellowships are part of a bold vision to challenge colleges, universities, businesses and other stakeholders committed to advancing the field of computing to transform undergraduate computer education on a national scale." Also receiving a CISE fellowship was O. Astrachan of Duke University.

## Zombie Nets
## National Journal (07/14/07) Vol. 39, No. 28, P. 46; N. Munro

C. Painter of the Justice Department notes that countries with weak anti-cybercrime enforcement become hacker sanctuaries, which can thwart the track down of these criminals by US authorities, according to former Pentagon principal assistant secretary of Defense for networks and information integration L. Wells. Networks of compromised "zombie" computers, or "botnets," which can flood target systems with traffic, are being constructed and improved by malefactors as revenue-generating tools, say Painter and Arbor Networks' J. Nazario. Profits can be realized by using botnets to send spam or shut down competing companies' online sales, while zombies can also be employed to gather information about computer owners' finances and then fleece banks and credit card firms. Botnets have also served as political weapons, most recently to shut down Estonian government Web sites in protest of the country's decision to relocate a World War II monument. But many of the people behind botnets are based in countries outside of US jurisdiction - countries with little or no sanctions against cybercrime. Even miscreants in nations with strong anti-cybercrime laws can avoid apprehension by routing their online activities through systems in sanctuary states, say experts. "They assume they're not going to get caught, and looking at the odds, they're right," notes Nazario. This situation is spurring US officials to lobby foreign governments to enforce computer security and comply with directives such as the Council of Europe Convention on Cybercrime, which offers model computer-security ordinances.