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

**Δελτίο 101**
**8 Γενάρη 2008**

---

**FBI Prepares Vast Database of Biometrics**
**Washington Post (12/22/07) P. A1; E. Nakashima, R. Drezen**

The FBI has a target to build the world's biggest biometric computer database at a cost of $1 billion that would enable the government to identify individuals in the United States and overseas on an unprecedented scale. This system, known as Next Generation Identification, will compile diverse biometric data in one place for identification and forensic purposes, and supporters say integrating information from assorted sources and making it accessible to multiple agencies will boost the likelihood of apprehending wrongdoers. The FBI's Kimberly D. Greco says the database will "fuse" face, iris, fingerprint, and palm matching capabilities within six years, adding that privacy is protected by keeping audit trails on everyone with access to a record in the fingerprint database. For the past few years, the Defense Department has been electronically archiving images of fingerprints, irises, and faces of over 1.5 million Iraqi and Afghan detainees, Iraqi citizens, and foreigners who require access to American military bases, while the Homeland Security Department has been employing iris scans at certain airports to confirm the identity of travelers who have passed background checks and who wish to quickly move through lines. The growing utilization of biometrics as identifiers is bringing questions about the ability of Americans to avoid undesired surveillance to the fore, and critics argue that such projects should not go forward without clear evidence that criminals really can be spotted within crowds via biometrics technology. The German government carried out a scientific study on the effectiveness of face recognition in crowds this year and learned that the technology was still too ineffective for use by law enforcement authorities. The ACLU's B. Steinhardt warns that biometrics technology is "enabling the Always On Surveillance Society."

**Computer Security Expert Martin Abadi Garners Outstanding Innovation Award**
**UC Santa Cruz (12/21/2007), K. Schmidt**

ACM's Special Interest Group on Security, Audit, and Control (SIGSAC) has honored UC Santa Cruz computer science professor M. Abadi with its Outstanding Innovations Award. Abadi received the award for the significant contributions he has made in applying logic and provability to information security. "Dr. Abadi made key contributions to authentication in distributed computer systems, and to the design and analysis of security protocols for authentication," ACM said when it announced the award. "His published research has initiated entirely new productive directions that have attracted the contributions of researchers all over the world." A principal researcher at Microsoft Research, Abadi holds patents in the areas of distributed systems, programming language analysis, and computer security. He is also an editorial board member of the Journal of the ACM. Abadi received the award at the SIGSAC Computer and Communications Security Conference in Alexandria, Va., in November.

**Paper Ballots Go High Tech**
**St. Petersburg Times (FL) (12/26/07), B. Varian**

Following an electronic voting scandal, Florida now requires all counties to use optical scanners, a decades-old technology that satisfies the need for a paper trail, but the state is also using new technologies that could create several significant problems. As many as 27 counties in Florida plan on using ballot-on-demand machines to print ballots during early voting and for absentee ballots. The machines allow poll workers to print ballots customized to voters' precincts and party affiliations. Unfortunately, the machines could jam and be unable to print ballots, which would create a long line of voters. Ballot-on-demand machines enable poll workers to print out a person's district ballot type wherever he or she arrives to vote. Ballot-on-demand voting will also help save money, as counties no longer have to print out extra ballots to avoid shortages since they can be printed as needed. The ballot printers look very similar to office printers and copiers, which supports fears that the machines may jam or break down, which is why some supervisors are not rushing to deploy the technology. Orange County supervisor of elections B. Cowles plans on testing the equipment and examining several scenarios, such as if someone makes a mistake on the ballot and needs a new one and possible difficulties in printing multilingual ballots. "It works okay if it's just one person coming in at a time," Cowles says. "But when you start looking at early voting sites in a presidential year, you have to consider what's going to be the best way and most accurate way and fastest way to process a large number of voters."

**Wi-Fi Routers Are Vulnerable to Viruses**
**New Scientist (12/22/07), Z. Merali**

Indiana University in Bloomington researcher S. Myers has been investigating how a virus could be spread between wireless routers. "We forget that routers are mini-computers," Myers says. "They have memory, they are networked, and they are programmable." However, routers are not usually scanned for viruses or protected by firewalls, and while Myers says there are no known viruses that target routers, they are still easy targets. Routers within about 100 meters would be able to spread viruses to one another and create a vast network for viruses. While routers normally do not communicate with each other, it would be easy for hackers to create a virus that enables routers to communicate. Myers used records on the location of Wi-Fi routers around Chicago, Manhattan, San Francisco, Boston, and parts of Indianapolis to create a simulation of how a router attack might spread. In each simulated city, viruses were able to jump between routers lacking high-security encryption within 45 meters of each other. The virus spread surprisingly fast, with most of the tens of thousands of routers becoming infected within 48 hours. The geography of the cities affected how the virus spread, with rivers and bays acting as "natural firewalls." Routers can be protected by changing the password from the default setting and enabling high-security WPA encryption. University of Cambridge computer scientist Ross Anderson says the study exposes a more significant problem in that all electronics, including phones, routers, and even microwaves, are being built with software that could potentially become infected.

**Tests in Ohio Point to E-Voting Insecurities**
**Computerworld (12/31/07), T. Weiss**

Recent tests of Ohio's electronic voting systems exposed security shortcomings that are a continuing danger to the accuracy of elections, concludes a report released by Ohio Secretary of State J. Brunner. The report recommends several steps to minimize those threats, including centralizing the electronic voting counting and no longer using touch-screen voting machines. "These findings do not lend themselves to sustained or increased confidence in Ohio's voting system," Brunner writes in the report, noting that the e-voting machines "do not meet

computer industry security standards and are susceptible to breaches of security that may jeopardize the integrity of the voting process." Johns Hopkins University computer science professor A. Rubin, who heads the e-voting activist group ACCURATE, says that Ohio's security problems are so severe that it is not surprising they are trying to eliminate touch-screen machines. "I don't think it's impossible to build high-tech voting systems," Rubin says. "But it will require a lot more quality control and effort than we've seen so far."

**Electronic Passports Raise Privacy Issues**
**Washington Post (01/01/08) P. A6; E. Nakashima**

US citizens that travel frequently between the US and Canada or the Caribbean will soon be offered RFID-embedded passports that can be read from 20 feet away. The cards are intended to be more convenient for travelers but create security and privacy concerns due to the possibility of data being intercepted. The RFID passport card costs $45 and cannot be used for air travel, and citizens have the option of a $97 card that is more secure and can only be read at a distance of three inches. "The government is fundamentally weakening border security and privacy for passport holders in order to get people through the lines faster," says Center for Democracy and Technology deputy director A. Schwartz. Schwartz says the problem with using RFID for identification is that the technology was not designed to be secure or to track people, it was designed to track goods during shipping. The government says the chip will contain a unique identifying number linked to information in a secure government database but not to names, Social Security numbers, or any other personal information. The card will also come with a protective sleeve to prevent hackers from scanning data wirelessly. Schwartz says a reader with a strong battery could detect the chip's signal from as far as 40 feet away, and that the chip could easily be reproduced to fool a border agent. Last year, the Government Accountability Office reviewed technology similar to that being used in the passport cards and reported that the technology should only be used to track goods, not to identify people. The State Departments wants to being issuing the passport cards this spring.

**Human factors researchers test voting systems for seniors that can improve accuracy and speed for voters of all ages, Human Factors and Ergonomics Society (12/20/07)**

Florida State University human factors researchers T. Jastrzembski and N. Charness have identified ways to improve electronic voting accuracy among older voters while simultaneously reducing waiting time at polls. The researchers tested ballot and machine usability with a focus on older voters, who because of reduced vision and motor control can have a more difficult time using computers, particularly in a time-sensitive situation. Two subject groups, ages 18-26 years old and 64-77 years old, tested four ballot layouts and machine designs, including a touchscreen machine with a full ballot on a single screen, a touchscreen with one ballot per screen, a touchscreen and keypad with a full ballot, and a touchscreen and keypad with a single ballot. The touchscreen with a single ballot per screen produced the most accurate results, but the pure touchscreen with a full ballot had the fastest completion times. Jastrzembski and Charness recommend additional studies with older voters, which could lead to more user-friendly machines and ballots for users of all ages.

**Computer Terrorism Becomes a Concern**
**Patriot-News (PA) (12/25/07), G. Lenton**

Malware infiltration, no matter how minor, is a cause for concern among computer security experts across the US. In September the Government Accountability Office issued a report warning that the computer systems responsible for running the nation's infrastructure are increasingly vulnerable to hackers, and their disruption could seriously affect the national economy. In theory, electric service to a city or a region could be shut down by attackers who exploit poorly shielded home computers across the country. "If everybody who had a home computer would simply enable a firewall and make sure antivirus software was in place and put anti-spam components in their system, there would be a significant drop in what we see," argues chief information security officer for Pennsylvania R. Maley, whose office impedes 25,000 viruses, 10 million attempts to penetrate firewalls, and 80 million spam emails every month on average. Hackers are now motivated to compromise systems for profit rather than for bragging rights, and there are criminal gangs in Russia and eastern Europe that offer hacking services, according to Maley. Lehigh University professor M. C. Chuah notes that initiatives to enhance the security of government-controlled systems are gaining traction, but she thinks a greater effort to secure business systems that depend on Internet connections is required. Deputy director of reactor security at the Nuclear Regulatory Commission S. Morris says the increasing reliance on digital information has been accompanied by the growing importance of security.