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

Δελτίο 44
14 Οκτώβρη 2006

Lots of Processors Inside Everything
Electronic News (10/05/06), J. Davis

Inventor and author R. Kurzweil suggests that the exponential progression of technology signals the next natural step in biological evolution's progression. Kurzweil delivered a keynote address at the ARM Developers Conference in Santa Clara on Wednesday, October 5, 2006, in which he claimed that "we are moving towards an era where computers are not going to be discrete products. They will make their way into our bodies and brains and replace biological neurons." The latest generation of FDA-approved embedded neurons, which allow for the download of new software, is pointed to as evidence. His views are founded on the thought that technological and biological innovation progresses exponentially rather than linearly, doubling every year. Evidence of this biological progress is a study in which scientists were able to shut off the fat gene in animals, allowing them to eat tremendous amounts and not create fat stores. The fact that it took 50 years for the telephone to make its way into the hands of 25% of Americans, but search engines caught on in only 5-6 years, is also cited as proof of rate change in innovation. "Applications like cell phones are make the world a better place," says Kurzweil. The World Bank has recently noted that current technologies are helping to cut poverty rates in Asia over the past 10 years, and predicted that poverty would be cut by another 90% in the region over the next 10 years. Moore's law can be continued by Intel until 2022 says Kurzweil, but then it will be time for a paradigm shift. The next paradigm? He says it will be 3D. "When I postulated the idea in my last book on the subject it was a radical notion. It's a mainstream idea now." The combination of biological and technological innovation, Kurzweil explains, will lead to an attitude of "treat[ing] biology as information technology and use information technology to reprogram it." A simulated human brain will be possible by 2013 and cost only $1,000, says Kurzweil.

Pennsylvania Voters on E-Voting: Trust, But Verify
AScribe Newswire (10/04/06)

A late September survey done by two different Pennsylvania colleges reveals an overwhelming majority in support of paper verification in e-voting. Over 80% of those surveyed at Lehigh University and the Muhlenberg College Institute of Public Opinion agreed that verification was necessary, a statistic that covered all demographics. Those surveyed were found to have far less trust in e-voting machines than ATMs but more faith in e-voting machines than making secure purchases online or being properly screened at the airport. Although the majority feels that voting machines have been tested correctly and would be free from fraudulent activity, over a third believe that it would not be difficult to tamper with results, and nearly two thirds do not have faith that their vote would be properly counted. These results reveal a great awareness of election fraud, and a basic caution toward technological innovation. "It is reassuring to see that the warning flags raised by the computer security community have not been missed, at least by voters," says D. Lopretsi, an associate professor of computer science and engineering at Lehigh and an e-voting expert. Another contributor, Z. Munson, professor of sociology at Lehigh, said "the results indicate that the adoption of voter verified paper au-

dit trail systems will be important to the public's trust of the country's democratic process in the coming years," and adds that concern over voter fraud is present in both parties.

UTSA Awarded $3.1 Million for Cyber-Security Program Development
EurekAlert (10/04/06)

A three-year, $3.1 million competitive training grant has been awarded to the University of Texas San Antonio Center for Infrastructure Assurance and Security (CIAS) as an extension to a $1 million grant given by the Dept. of Homeland Security (DHS) in order to aid state and community efforts to build cyber-security training and development programs. The grant is a reward for the center's efforts to help state and local governments in the prevention of cyber-terror attacks. CIAS is built upon cooperation between academia, the information technology industry, and the local Air Intelligence Agency. Technical and policy issues concerning information assurance and security, as well as the task of security training, are taken on by the center. In 2002, the center led the successful "Dark Screen" exercise in defending against cyber-terror attacks, as part of the DHS' CyberStorm exercise. As a result, the city of San Antonio was recognized as the first in America to carry out a cybersecurity exercise. "As one of only three DHS training partners in the nation working in cybersecurity, we feel this increased funding supports our efforts to lead and develop models that DHS can recommend states and communities to adopt," says CIAS director Fred White. Over the past five years, over $12 million in Defense appropriations bills has been awarded to UTSA's CIAS in order to support community cybersecurity exercises and research. In addition to holding several collegiate cybersecurity competitions, CIAS has worked in several communities outside of Texas, including infrastructure security and assurance for telecommunications, oil and gas communities and the chemical sectors in San Francisco, New York, Chicago, Miami and Baltimore.

Online Elections Would Attract Younger Voters -- Someday
San Francisco Chronicle (09/30/06) P. A2; C. Nevius

Despite significant increases in youth voting witnessed in primaries featuring online voting in Michigan in 2004 and Arizona in 2000, the country still appears a long way from being able to vote in a general presidential election from home. C. Smith, former director of online voting service Election.com, which ran the Arizona primary, says "60% of the younger generation would vote [if it was possible online]. That is based on our test trials." The number of voters aged 18-30 jumped from 1,708 in the 1996 Arizona Democratic primary to 7,760 in the same primary in 2000. This turnout was the largest for a primary since 1984, when the Democrats began holding primaries. Arizona became the first state to institute online voter registration in 2004 with its "EZ Voter" plan, which has been even more successful than predicted. Half of the current voter registrations in Arizona were done online. Michigan saw one-third of all votes cast via the Internet in its 2004 democratic primary. Despite this irrefutable evidence that it would increase voting, the dangers involved in using the Internet cannot be ignored. Computer science professor A. Rubin says that "we'd have to completely redesign what computers are and what the Internet is" in order to make online voting a reality. Rubin warns that a virus could be created to cast thousands of illegal votes, or simply shut down voting in parts of the country. Smith does not agree that safety is such a concern at this point. His evidence is that experienced hackers were hired to try and disrupt the Arizona primary, and while one was able to, all that occurred was that the system shut down for about one minute, and then the hacker had to "go back for another 8 hours to try to get in." Experts convinced the Pentagon to cancel a program in 2004 that would have allowed troops overseas to

vote online because of the threat of sabotage. Even those who zealously support the cause of online voting admit that it is no less than 10 years away.

Neither Safe Nor Secure on the Internet
CNet (10/04/06), J. Archer

Although some believe the domain name system (DNS) should be allowed to operate without "burdensome" oversight, the Internet will not be very safe or secure without the adoption of some reasonable rules of the road included in the pending proposals to operate top-level domain (TLD) registries, writes J. Archer, the managing director of Devonshire Enterprises. Archer points out that despite attacks on the DNS, ICANN has failed to provide these "rules of the road" for the operators of the proposed registry agreements for the .com domain with VeriSign and the proposed .biz., .info, and .org TLDs. Archer adds that ICANN has instead opted to allow VeriSign and other registry operators to make up and freely change their own security rules, not to tell the public or ICANN these rules, or to disclose how well their rules are working. In addition, the proposed .com registry agreement now pending before the US Dept. of Commerce would allow VeriSign to do as it sees fit, Archer writes. Though VeriSign has in the past seen fit to develop robust security, the company could someday decide to sacrifice some security for additional profits, he adds. Archer concludes that ICANN should be given the authority to prevent this from happening.

Cut the Ties That Terrorize
InformationWeek (10/02/06)No. 1108, P. 56; E. Chabrow

The Dept. of Homeland Security, in a move that has provided a temporary answer to its critics who say it is shirking its responsibility to protect against a terrorist attack on the Internet, has appointed Gregory Garcia as its first assistant secretary for cybersecurity, a position that has been vacant for 14 months. Attacks have occurred recently, though not the "big one." A coordinated denial-of-service attack disrupted 13 domain-name root servers and made several Web sites unavailable. In early 2006, a hacker brought down 1,500 Web sites by hijacking PCs and sending traffic to servers with a DNS query and forged source address. G. Foresman, undersecretary for preparedness, says the role of Homeland Security "isn't necessarily to do it all, but to make sure we get all the players to the table and make sure it all gets done." No success can be achieved without cooperation from the private sector. Private firms are unwilling to divulge critical network information because of fear it could be leaked to competitors. D. Powner, GAO's director of IT management, says, "right now, with the folks we talk to in the private sector, they don't see a lot of return from the Dept. of Homeland Security. There are real leadership issues there." The GAO complied a list of 13 key cybersecurity responsibilities for the department, yet none have been addressed completely. One item on the list is "develop and enhance national cyberanalysis and warning capabilities." While the threat of a massive attack looms, even slight tampering, perhaps in the realm of medical records, could cause a devastating loss of confidence in electronic intelligence. The Internet Security Alliance says that every day $3 trillion moves across network connections protected by a 30-year-old protocol that has many known security weaknesses, while in 2004, the Congressional Research Service estimated that businesses have lost $226 billion as a result of cyberattacks.

Standards to Stimulate E-Voting?
CNet (10/06/06), C. Lombardi

The CalTech/MIT Voting Technology Project at the Massachusetts Institute of Technology last week convened a panel of election and data specialists to discuss the challenges of incorporating technology into the voter registration process in order to assure accuracy and maintenance. A major problem identified by the panel is a lack of standardization in the way that voter information is stored. The way in which first and last names are broken down in some registries while being lumped into a single name in others was cited as one obstacle. Suffixes such as Jr. and Sr. only add to the confusion. The Help America Vote Act of 2002 included no such rules or recommendations for standardization. A system known as Texas Election Administration Management (TEAM), scheduled to be operational by 2007, is accessible via the Internet and allows local changes to state ballots. The service allows a voter's information to be transferred within the state should they move, but before such a system can be implemented, the old data must be cleaned up. Current possibilities for exchanging data between states include Election Markup Language (EML) and Extensible Markup Language (XML). TEAM uses an XML-based format called EDX; 254 of Texas's counties have chosen to implement TEAM, but 27 have chosen to remain offline. Meanwhile, an unwillingness to join the e-voting trend is causing problems for the standardization efforts as some districts prefer their own, traditional, systems. Panelist Thad Hall, a professor at the University of Utah and co-author of "Point, Click, and Vote: The Future of Internet Voting," compared this reluctance to the VHS vs. Betamax debate where consumers sat back and waited to see which format would gain prominence. "I am confident that three or four years from now, everyone will come online," said panelist A. McGeehan, director of elections for Texas. The Healthcare Insurance Portability and Accountability Act is cited as a success of standardization; where 450 formats were condensed into a single standard in six years.

Flaw Found in European Voting Machines
IDG News Service (10/06/06), R. McMillan

Electronic voting machines used by 90% of Dutch voters can be easily tampered with, says Dutch e-voting researchers in a report published Friday. The researchers say, "We don't trust voting computers. Anyone, when given brief access to the devices at any time before the election, can gain complete and virtually undetectable control over the election results." Radio emanations can be studied to find out what votes were being cast, according to the researchers, who also claim that all that is needed to break into theWedap/Groenendaal ES3B voting machine, the same type used in France and Germany, is a key that can be purchased on the Internet. The same type of key is also available for the Diebold voting machines used in the US, according to E. Felten, the director of Princeton University's Center for Information Technology Policy. Felten and his colleagues conducted a test in which they claim to have been able to install vote-altering software on Diebold's AccuVote-TS machine in less than a minute. While Diebold disputes these claims, Felten calls the security problems facing e-voting "very difficult or even infeasible to address." The manufacturer of the voting machine used in the Netherlands, Nedap, claims that it is significantly more difficult to tamper with the results of an e-voting system than a paper ballot system. When asked if manipulation of their machines was possible, the company responded, "everything can be manipulated."

$100 Laptop May Be at Security Forefront
Associated Press (10/09/06), B. Bergstein

In creating the $100 laptops planned to be distributed to 7 million children around the world, software developers have instituted groundbreaking security measures. The developers working on the One Laptop Per Child project envision a computer that does not need virus protec-

tion, because applications are run in a "walled garden," meaning that an application does not have access to all files on the computer, unlike conventional systems that are vulnerable to exploitation, theft or erasure of information. "It's essentially unbelievably difficult to do anything to the machine that would cause permanent hardware failure," says I. Krstic, a software architect at One Laptop Per Child who focuses on security. The specialized encryption technology serves as a security back up, preventing the BIOS software, which runs when the computer is first turned on, from being overwritten, thus the computer could not be made unbootable. When the machine enters the child's school's wireless range, all data will be backed up on a server. While these measures are believed to be effective, children can tweak the computers and learn how they operate, meaning they could potentially turn off the security measures. One thing that could worry developers is the fact that the machines will be able to interact in a "mesh" network, sharing data and programming code, but Krstic promises that this element would be "really scary if we were not paying attention to it...But we think we have solutions to all of these problems." The bright-colored, hand-cranked, wireless-enabled laptops will be distributed in Thailand, Nigeria, Brazil, and Argentina.

Tactile Passwords Could Stop ATM 'Shoulder Surfing'
New Scientist (10/06/06), T. Simonite

A new system for entering a PIN number at the ATM is being developed using a system based on feel rather than sight. The practice of "shoulder-surfing," where someone watches numbers typed by an ATM user, is the target of new technology being devised by computer engineers at Queen's University in Belfast. Users would move a pointer over a grid of nine blank spaces displayed on the ATM screen using their fingertips. When they pass over a different box, the tactons beneath their fingertips change. When the user comes across each specific pattern of their code, they click. "The tactile displays are under you fingertips so there's less chance of an observer "shoulder-surfing," says R. Kuber, who created the system with colleague Wai Yu. Rather than remembering a number, ATM users would have to remember the feel of four distinct patterns made up of nine pins that can create many unique patterns. "Even if someone tried to share their information, there's no guarantee another person could replicate it," says Kuber. The feasibility of this technology is being tested. In one study, 16 subjects used the tactile system to log into their computers everyday for two weeks, and were able to remember their code after two weeks of not using it and sign in by the second attempt, but the average sign in time was 38 seconds. "Finding patterns that aren't too hard to identify is the biggest problem...an array of nine pins is crude compared to our sense of touch, there's no reason the hardware couldn't be improved," Kuber says. The system was presented last month at the British Computing Society's Human Computer Interaction Group conference at Queen Mary of London.