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

**Δελτίο 70**
**20 Απρίλη 2007**

### Protecting Electronic Information From Theft and Abuse Is the Goal of Virginia Tech CAREER Research, Virginia Tech News (04/09/07)

Virginia Tech researcher P. Schaumont has been awarded a prestigious NSF grant to fund his efforts to improve information security in computing devices. The NSF Faculty Early Career Development Program (CAREER) Award is the top honor given to promising young researchers and includes a five-year, $400,000 grant. Schaumont says that as more and more information is being stored on portable computers such as an electronic key fob used to unlock a car door or the image of a signature on an electronic passports, encryption technology has not kept up to protect data stored on portable devices. "Computers of all sizes can be stolen," says Schaumont. "The way we use computers everyday is changing, so we need to rethink how to safely store information." He intends for his CAREER project to produce a methodology by which secure embedded systems can be designed. Such innovation would allow protection of information in cell phones, RFID, and copyrighted materials, such as audio files on portable devices. For the mandatory educational element of his CAREER project, Schaumont plans to expose students to hardware-software co-design--the development of hardware and software in an embedded system.

### Biggest Threat to Internet Could Be a Massive Virtual Blackout
### National Journal's Technology Daily (04/05/07), A. Noyes

A distributed denial of service attack presents the biggest danger to the Internet in the 21st century, according to ICANN's S. Crawford. Speaking at a Hudson Institute briefing, Crawford said the Feb. 6 zombie attack on six root-zone servers called attention to the fact that such servers have little or no oversight. To reduce the risk of DDOS attacks, the number of zombie computers must be reduced, but "people are turning millions of PCs into weapons ... and we don't have a lot of data about what is happening," said Crawford. "Researchers are often operating in the dark." DHS has shown an inability to address this danger, she added. "They're trying, but many of their efforts lack timeframes for completion." Crawford does not believe legislation could prevent DDOS attacks, because Congress' reach "is too local for the networked age." The best solution would be to focus money and attention on potential global educational initiatives, perhaps through the founding of a multi-stakeholder body with a "new, friendly-acronym," she said. ICANN's power is overly based on contracts and is not wide enough to have the necessary impact, and the Internet Governance Forum is "highly political" and "not necessarily the best forum for a technical discussion of best practices," claimed Crawford. She named routing security as an important future consideration, because the ability of hackers to place false paths in a routing system to obtain packets or spur a DDOS attack increases as "routing tables" grow in size to meet the needs of IPv6.

### Don't Trust Voting on the 'Net, Speaker Says
### Network World (04/12/07), T. Greene

While giving the keynote address at the Usenix symposium on networked system design and implementation, Massachusetts Institute of Technology computer science professor R. Rivest said Internet voting is so vulnerable to manipulation that it should be avoided unconditionally, calling Internet voting "voting by mail made worse." Like voting by mail, Internet voting creates the possibility of voter fraud, as well as possible voter intimidation and coercion, as privacy cannot be guaranteed with Internet voting as it can in a voting booth, according to Rivest. Electronic voting without the use of the Internet has enough problems, including voting machine security, millions of lines of private code, and voting machine networks that could be vulnerable to machine tampering through the network or denial-of-service attacks. Rivest said the source code for voting machines, and their underlying operating systems, should be given security checks by testing labs. Rivest said there is a significant gap between voting-system theories and a real-world voting system that the public will trust, saying it can take 15-20 years for the public to understand how systems work.

### Researchers Explore Scrapping Internet
### Associated Press (04/15/07), A. Jesdanun, A. White

Some university researchers believe the only way to truly create a secure Internet is to take a "clean slate" approach and build the architecture of the Internet all over again, an idea that has gotten some support from the federal government. Rutgers University professor, and project manager on three clean-slate projects, D. Raychaudhuri said the Internet was designed for different purposes than how it is currently being used, and it is "sort of a miracle that it continues to work well today." The Internet's early architects designed and built the system primarily on trust, as they largely knew each other, and consequently designed a network intended to be kept open and flexible. New threats, like spammers and hackers, are able to exploit that open network, and recently developed security features add complexity and reduce performance. A major challenge to any effort to rebuild the Internet will be determining the role different organizations play in its construction, as the first time researchers in labs were largely responsible for original developments, but now the government and law enforcement will want to play a far more significant role. Meanwhile, the National Science Foundation's Future Internet Network Design program is funding research on the Global Environment for Network Innovations (GENI), an experimental research network. Rutgers, Stanford, Princeton, Carnegie Mellon, and MIT are among the universities pursuing individual clean-slate projects, as is the Department of Defense and the European Union, though any results from these projects are not expected to arrive for another 10 to 15 years. "Almost every assumption going into the current design of the Internet is open to reconsideration and challenge," said NSF's G. Parulkar, who is leaving to become executive director of Stanford's clean-slate initiative. "Researchers may come up with wild ideas and very innovative ideas that may not have a lot to do with the current Internet."

### Expert: 'Flasher' Technology Digs Deeper for Digital Evidence
### Purdue University News (04/12/07), K. Medaris

R. Mislan, Purdue assistant professor of computer and information technology and former US Army electronic warfare officer, said a technology currently in use in Europe could potentially be used to help solve thousands of cybercrimes in the United States. The "flasher box" can be used to download and analyze every bit of information from a wide variety of cell phones, a huge advantage over current forensic techniques that requires investigators to issue specific commands and receive only information relating to the command. With the flasher box, investigators can download the entire contents of a cell phone for examination, including call history, text messages, contacts, and deleted images and videos. "Using a flasher box is like taking a snapshot of the cell phone," Mislan said. "This method shows a lot of promise." The content of the phone is downloaded and appears as a stream of letters and numbers that only requires a mathematical translation to turn the code into useable information. Mislan said the key to success with flasher boxes is finding the correct software and cables to match the wide variety of phones available on the market.

### Analysis: Owning the Keys to the Internet
### United Press International (04/12/07), S. Waterman

The US government is moving ahead with its plans to create a new security system for the Domain Name System (DNS), despite concerns from international Internet management companies. The DNS directs Internet users to the sites they want to visit by translating URLs into numerical Internet Protocol (IP) addresses, but because the DNS was built with a relatively open structure, criminals can use techniques known as DNS "spoofing" or "poisoning" to create duplicate Web sites to steal information from users who think they are logging on to their bank or email accounts. The DNS Security Extensions Protocol (DNSSec) is intended to create instantaneous authentication of DNS information, eliminating the opportunity for DNS abuse and essentially creating a series of digital keys for the system. The question that many groups are asking is who should control the key for the DNS Root Zone, the part of the system that is above top-level domains such as .com and .org. The US Department of Homeland Security, which is funding the development of a technical plan for implementing DNSSec, issued an initial draft in October that essentially narrowed potential Root Zone Key operators down to a government agency or a private contractor, though no specific organizations were listed. A new version of the draft specification for the DNSSec plan that incorporates input from experts could be ready by the end of this summer, says D. Maughan of the Department of Homeland Security's Science and Technology Directorate. Canadian Internet Registration Authority President Bernard Turcotte and others are concerned the US would unilaterally implement DNSSec. "We want to ensure that whatever measures are implemented are well coordinated," Turcotte says. Maughan says the US government is committed to using DNSSec within the .gov domain, but he says "it will take a lot more people to get involved" to globally deploy DNSSec.

### Open-Source Project Aims to Erase E-Voting Fog
### IDG News Service (04/16/07), J. Kirk

University College Dublin computer science lecturer J. Kiniry believes that e-voting is risky and available software systems are substandard, saying governments feel obliged to use e-voting to feel modern, despite computer security experts' warnings that e-voting is insecure. Kiniry knows governments are going to forge ahead with the implementation of e-voting systems, so he and a team of researchers designed an open source e-voting software system that he hopes will create a secure foundation for e-voting. In Kiniry's system, voters register at a government office and receive a PIN. Later, the voter will receive a unique ballot in the mail, and on election day, the voter will enter their voter ID code and PIN on the Web site. To select a candidate, the ballot has a number next to each candidate that is different for every voter, a type of pre-encryption, ensuring that the number can only be used once and will be useless if intercepted. Kiniry's system also provides the voter with a receipt number to make sure the vote was counted. Recounts remain a problem because there are no physical ballots, and like other systems, a recount would entail the system running the same software over again, which is not an acceptable solution according to Kiniry. Kiniry believes a possible solution would be to allow a third party to develop their own software that could be used for recounts, but because elections have such ambiguity without computer technology, it is likely any electronic voting system will have ambiguities as well.

### Docs Point to E-Voting Bug in Contested Race
### Wired News (04/17/07), K. Zetter

Incident reports from a controversial election in Sarasota County, Fla., last November show that poll workers from at least 19 precincts contacted technicians and election officials to report touch-screen sensitivity problems, symptoms associated with a known software flaw in the I-Votronic voting machine made by Election Systems & Software (ES&S). County officials claim the election results were not altered by the bug, but activists are arguing that the flaw might have contributed to the high number of lost or uncast votes in what is now a highly contested and controversial election. Voters complained of having to press the touch screen harder and multiple times to register a vote, a symptom similar to one caused by a bug the machine's maker revealed prior to the election but was ignored by the county. The incident reports also cited problems during the primary election two months earlier, a contradiction to a statement made by Sarasota supervisor of elections Kathy Dent, who said no such problems occurred during the primary. ES&S sent a sign to be posted in polling places instructing voters to hold their finger on the screen until their selection was highlighted, which could take several seconds according to the sign. Dent chose to post a different sign listing steps for casting a ballot and encouraging voters to check the review screen at the end of the ballot for accuracy, but the replacement sign made no mention that voters may need to hold their finger to the screen for several seconds. In the election, Republican V. Buchanan won over Democrat C. Jennings by fewer than 400 votes, and more than 18,000 ballots recorded no vote in the race. Jennings is now contesting the results in court, and the House Administration Committee has formed a special taskforce to investigate the election.

### Dartmouth Gets Award for Cyber Security Studies
### Dartmouth News (04/13/07), L. Burnham

Dartmouth is set to receive more funding from the US Department of Homeland Security that will enable its Cyber Security Collaboration and Information Sharing Project to further study cyber security. The Institute for Information Infrastructure Protection (I3P) will receive $8.7 million to conduct new studies on insider threats, privacy protection, and the economics of cyber security, and the Institute for Security Technology Studies (ISTS) will receive $3 million and continue its research into security and privacy matters. "ISTS is excited to initiate several research projects that will develop cutting-edge technologies, including sensor networking, autonomic computing, video forensics, and public-key infrastructure," says ISTS executive director D. Kotz. "Addressing real-world problems related to cyber security and infrastructure requires a multidisciplinary approach," says I3P Chair M. Wybourne. "The unique character of the consortium enables faculty and students from many disciplines to join forces to further our understanding of the issues." Both institutes will also put some of the funds toward educational programs, seminars, and workshops for students.

### Security Remains a Challenge for Browser Developers
### eWeek (04/17/07), P. Galli

At the Web 2.0 conference this week in San Francisco, leading companies in the Web browser industry, ranging from open-source communities to software powerhouse Microsoft, addressed the arrival of Web 2.0 and what effect it would have on Web browsers, and everyone agreed that security was one of the biggest challenges facing the industry. C. McCathie-Nevile, the chief standards officer at Opera, said security models on the Web are immature, and that Web browser developers are committed to interoperability and what users want, not starting another browser war. Microsoft's Chris Wilson, platform architect for Internet Explorer, admitted that Web browsers still have a long way to go. "They are all missing some of the client-side features, but have certainly become far more robust over time," Wilson said. When asked what spurred the development of Web 2.0 applications, Wilson said social networking and mashups were widely responsible, but Mozilla's chief technology officer B. Eich said development tools were helpful. Eich said current efforts are focused on making memory use more linear, but this type of development takes time.

**Feds: Accuracy of Face Recognition Software Skyrockets**
**LiveScience (04/13/07), L. Wood**

Face recognition software is 20 times better than it was five years ago, according to the National Institute of Standards and Technology. In NIST's latest results from its Face Recognition Vendor Test, the best face recognition algorithms had a rate of false rejections of 1%, compared with a failure to make correct comparisons 20% of the time in 2002. Speed is not a key characteristic of the algorithms, which make use of the single comparison approach, rather than compare every face in a database to every other face. "We fed the algorithms lots of data to get a statistically meaningful answer," explains J. Phillips, an electrical engineer who directed the test. "Our goal was to encourage improvement in the technology, and provide decision makers with numbers that would let them make an educated assessment of the technology itself." With random lighting on each face, the rejection rate was about 12%, compared with 20% five years ago.