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

Δελτίο 89
4 Σεπτέμβρη 2007

Official Threatens to Fine E-Vote Firm
Contra Costa Times (CA) (08/22/07), S. Harmon

California Secretary of State D. Bowen on Tuesday threatened to fine Election Systems & Software nearly $15 million and ban the company from doing business in California for three years for possibly selling as many as 1,000 uncertified machines to five California counties. Bowen accused ES&S of illegally selling 972 uncertified AutoMARK version 1.1 machines. The AutoMARK version 1.0 is a certified machine and is used by disabled voters in 14 California counties, including Los Angeles. If Bowen finds ES&S made unauthorized changes to the AutoMARK machine in version 1.1, she could ask a court or an administrative judge law to impose a $10,000 fine per violation, a total of $9.72 million, as well as a refund of nearly $5 million for the $5,000 machines. Bowen first became aware of the possible new version when ES&S applied for certification of a system that was already in place in five counties. If ES&S is banned from doing business in the state, counties that use ES&S machines would have to switch to another vendor, though Bowen plans to use the funds from the fines to help counties replace ES&S machines. An ES&S spokesman did not directly address Bowen's accusations, but said the company will work with her and that ES&S has a long history of complying with extensive and thorough examinations of its voting technology.

Japan Working to Replace the Internet
Kyodo News (08/20/07)

Japan plans to develop a next-generation network that would replace the Internet. Y. Suga, Japan's communications minister, says an organization that will bring together business, academic, and government interests will be established this fall. The group will head the efforts to pursue research and development for the new network. The ministry sees the Internet as lacking in data throughputs and security. The new network, which could be ready for commercial use in 2020, would be faster, offer more reliable data transmission, hold up better against computer virus attacks, and suffer fewer breakdowns. Japanese officials also see the initiative as a way for the nation to take the lead in developing new Internet technology and setting global standards, which they hope will better position local hardware and software providers in the global market.

Most Teen Computer Hackers More Curious Than Criminal
USA Today (08/20/07) P. 5D; M. Elias

Teenagers mostly commit cyber crimes due to curiosity and not criminal motivation, said University of San Francisco psychologist S. McGuire at the American Psychological Association conference. A survey of about 4,800 San Diego-area high school students revealed that 38% copied software illegally, while 18% accessed someone's computer or Web site without permission. However, only about one in 10 students said their intentions were for causing trouble or making money, while several cited the excitement and challenge as their motivation. Additionally, boys were more likely than girls to participate in hacking and make unauthorized software copies. "In the vast majority of instances, it's not a crime because it's not done with criminal intent," says University of Illinois in Chicago researcher S. Jones. He adds that parents should play a more active role in educating teens about the peril of copyright issues online and that they should also trust their children. N. Willard of the Center for Safe and Responsible Internet Use says most kids hack "just to see if they can do it" and that schools should implement programs pairing students with industry professionals that foster and promote positive PC activities.

Flight Plan for Security
Government Computer News (08/13/07) Vol. 26, No. 21, W. Jackson

S. Goodman of the Georgia Institute of Technology argues that the IT community must take a proactive stance toward securing cyberspace, and suggests using the Civil Aviation Convention as a prototype. The convention, to which nearly every country belongs, concentrates on standardizing rules for guarding the aviation infrastructure, and mandates operational competence in participating countries. As a result, the aviation industry is relatively safe despite its innate risks and high target profile. Meanwhile, the current information infrastructure was designed to be easily accessible, and "access is the enemy of security," according to Goodman. There are currently some 1.3 billion users of the Internet in over 220 countries. The majority of email traffic is spam, malware has infected roughly 14% of American household PCs, and today's global, interactive networks have no single source of authority or control. While the Council of Europe's Convention on Cybercrime is attempting to address such issues, its emphasis on law enforcement is too passive, says Goodman. Moreover, the convention does not insist that member countries create strategies for enforcing its regulations. In comparison, the Civil Aviation Convention insists that participating countries be able to fulfill and enforce its safety standards. A similar scheme in the cybersecurity world may find a helpful vehicle in the International Telecommunication Union, suggests Goodman.

Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates
Wired News (08/29/07)

Documents recently declassified under the Freedom of Information Act indicate that the FBI has constructed a point-and-click surveillance system capable of instantaneously tapping into almost any communications device. The Digital Collection System Network (DCSNet) links FBI wiretapping stations to switches run by landline operators, Internet-telephony providers, and cellular companies. The system consists of software that captures, filters, and stores phone numbers, calls, and text messages, and directly connects FBI wiretapping rooms throughout the nation to a wide-ranging private communications network. The outposts are connected via a private, encrypted backbone that is independent of the Internet and is run by Sprint for the government. Telecoms' installation of telephone-switching gear that meets wiretapping standards was mandated in 1994 with the passage of the Communications Assistance for Law Enforcement Act (CALEA), thus giving the FBI the ability to log directly into the telecom's network. CALEA's coverage was recently extended to require broadband ISPs and certain VoIP companies to enable their networks for federal wiretapping. Since telecoms became more wiretap-friendly, the volume of criminal wiretaps rose 60% from 1,150 to 1,839 in the past 10 years, and in 2005 92% of those wiretaps targeted cell phones, according to a 2006 report. CALEA wiretaps and the processing of all calls collected by DCSNet have racked up substantial costs, and security experts are worried that the system introduces new vulnerabilities to the telecommunications network. The declassified documents point to numerous flaws in DCSNet that Columbia University computer science professor S. Bellovin finds appalling, especially because they indicate the FBI is ignorant of inside threats. "The underlying problem isn't so much the weaknesses here, as the FBI attitude towards security," he says.

Research at K-State, Partner Institutions, to Help Homeland Security Make Sense of the Abundant Information in the Public Domain, Kansas State University News (08/27/07), E. Barcomb-Peterson

Kansas State University associate professor of computer and information sciences W. Hsu and other computer scientists with expertise in data mining are contributing to a project to develop technology that would make automated Internet searches simpler and more productive. "We're helping to develop the next generation of Web search and crawling," Hsu says. "The Dept. of Homeland Security wants to pull information that's available to anyone in the public domain, like millions of articles from sources like CNN and Al-Jazeera, and monitor them for security." Hsu's work for the Dept. of Homeland security project will focus on eliminating ambiguity in Internet searchers, including improved name recognition. The goal is to create a search engine that could, for example, differentiate between homeland security as a concept and Homeland Security as a government agency. "The goal is to develop an automated system that can pick out al-Quaida as an organization, Kandahar as a place, and Osama bin Laden as a person, based upon rules developed from previously-seen documents," Hsu says. The research will also work on solving another problem with finding information on the Internet--inefficient crawling. Search engines provide up-to-date results by looking through Web pages and archiving them, a process known as crawling and sometimes referred to as "crawling in the dark." Hsu says research in this area could create search engines that could anticipate keywords and create virtual neighborhoods of information by making connections between bits of information based on the results of similar searches.

US Suspends Vast ADVISE Data-Sifting System
Christian Science Monitor (08/28/07) P. 1; M. Clayton

The Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) system was used from 2004 to mid-2006 by the US Dept. of Homeland Security as a data-mining tool to hunt terrorists, weapons of mass destruction, and biological weapons using Americans' personal data and with little regard for federal privacy laws. Now, the $42 million system capable of processing trillions of pieces of data has been put on hold and may be terminated following data-privacy reviews, according to a report submitted to Congress by the DHS' Office of Inspector General (OIG). The OIG found that ADVISE failed to account for federal privacy laws during its design, and the system used live data, including personally identifiable information, from multiple sources without taking steps required by federal law, and DHS' own internal guidelines, to prevent the data from being misused. The failure to implement privacy safeguards in the ADVISE program appears to be the result of confusion and miscommunication about privacy requirements by ADVISE program managers and the DHS' privacy office. The privacy office argues that until the ADVISE system was connected to data it was not a data-mining program that needed privacy review. However, unknown to the privacy office, the ADVISE pilot programs had been operational and using real personal data for about 18 months before the privacy office made the report to Congress, the OIG discovered. The DHS has not disclosed what type and how much personal data was used, but DHS science and technology directorate spokesman L. Orluskie acknowledges that ADVISE may have been "too zealous in its testing." Orluskie says the ADVISE system is back on track, though he is unsure if the privacy assessment was complete or if operation had resumed. The damage may be done however, as the failure to follow privacy laws has reduced interest within the DHS in ADVISE, the OIG reports.

UM Study: Password Protecting Your Wireless Network Is Not Enough
University of Maryland (08/22/07), M. Corley; R. Copeland

Password protecting a wireless network may not provide enough security for home networks and is definitely insufficient for larger organizations' networks, according to a new by the A. James Clark School of Engineering at the University of Maryland. Wireless users that routinely look for access to any network available create a significant security risk as these wireless "parasites" can expose the network and all of the computers on it to a variety of security breaches. The problem gets even worse when someone authorized to use a wireless network adds an unauthorized wireless signal to increase the main network's signal strength, as these access points are particularly vulnerable and are often completely unprotected. Frequently, employees will set up their own wireless network, linked to the official network, to boost signal strength in their office, creating an unmanaged wireless access point. "If these secondary connections are not secure, they open up the entire network to trouble," says UM assistant professor of mechanical engineering and leader of the study Michel Cukier. "Unsecured connections are an open invitation to hackers seeking access to vulnerable computers." Cukier suggests network administrators limit signal coverage and disable Service Set IDentifier broadcasting so it cannot be detected outside the office or home. Additionally, Cukier suggests using either Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) encryption and regularly changing the encryption key.

America's Hackable Backbone
Forbes (08/22/07), A. Greenberg

By hacking into a nuclear power station, IBM researcher S. Lunsford demonstrated to the plant's initially skeptical owners exactly how vulnerable their supervisory control and data acquisition (SCADA) software was to attack. SCADA systems are employed nationwide to manage infrastructure such as natural gas and oil pipelines, water filtration, and trains. Moreover, the system's flaws are increasingly linked to the Internet, exposing a large swath of national infrastructure to any hacker with a laptop. Tipping Point security researcher G. Devarajan has notified SCADA software manufacturers about the weaknesses he has found, adding that though the bugs are simple, they are perilous. One such vulnerability enables hackers to insert their own commands, which would enable the insertion of false data. Still, the overwhelming complexity of critical infrastructure systems may be preventing criminals from controlling SCADA systems. However, over the past two years, threats have come in from hackers demanding ransom and claiming to have broken into SCADA systems, says A. Paller of the SANS Institute. The dearth of security features in SCADA systems can be attributed to their age, as most were created before infrastructure systems were linked to the Internet. In addition, many SCADA software developers fail to provide security patches, or make it hard to install such patches. J. Christy of the Dept. of Defense believes SCADA systems are in need of regulation by the government so that changes are made to increase security to at least a minimum standard.

A New Method to Detect Software Theft
Informationsdienst Wissenschaft (08/23/07)

Comparing the behavior of software programs is one way for companies to determine whether their software has been incorporated into other programs. Researchers at Saarland University in Germany have developed a tool, API Birthmark, which allows users to run their own program and a foreign program, analyze their behavior, and find similarities. A high degree of similarity detected by API Birthmark would suggest that code theft likely occurred, and that further investigation should be considered. The approach is different from other detection methods that focus on the code of the program, which can be easily obfuscated without destroying it, making it difficult to prove in court that software theft occurred. However, it would be difficult to change the behavior of a program without breaking it, similar to a birthmark. D. Schuler, V. Dallmeier and C. Lindig have written a paper on the birthmarking technique, which was accepted for the Automated Software Engineering (ASE 2007) conference in Atlanta.

Hacktivism Attacks May Rise, Homeland Security Official Warns
Network World (08/22/07), C. D. Marsan

When discussing implications of the Estonian cyberattack, M. Witt, deputy director of the US Computer Emergency Readiness Team, shies away from the term "cyberwarfare" and stresses the importance of preparation. The Estonian attacks showed the world the importance of cybersecurity, says Witt. Because the attacks involved financial targets, nations have realized that cybersecurity is not just essential to protecting critical infrastructures, but also homeland security and economies. Industry experts also noted that the attack was somewhat alleviated because Estonia's ISPs offered bandwidth greater than the size of the DoS attack. Witt notes that the US critical infrastructure has "a more robust type of backbone" than Estonia's critical infrastructure. That fact, combined with years of planning, means the US would react differently to a similar attack, says Witt. Witt acknowledges that the country is not completely secured from such an attack, but adds that plans have been established to handle attacks. Witt asserts that political attacks do not rank within the top three threats for US security networks. Rather, phishing and other socially engineered attacks are a major risk. Network operators should also be aware of the activity assailing their networks and firewalls, and should be aware of what is essential on the network and what the consequences will be if it is removed. Witt emphasizes training, noting that technical personnel must have enforceable policies in place in order to respond to attacks. Future U.S. CERT cybersecurity exercises include Zenith in 2007, which will be done with the Defense Department and Cyberstorm II, which will take place in March 2008 with the Department of Homeland Security. Cyberstorm II is an exercise at the national level, and will involve critical infrastructure representatives from across the country as well as from international governments.

Special Military Group Looks Ahead to Fight America's Future Wars
San Francisco Chronicle (08/26/07) P. E1; T. Abate

The Defense Advanced Research Projects Agency (DARPA) is looking to cutting-edge technology produced in Silicon Valley to fight future battles, and futurist P. Saffo noted at DARPA's recent 50th anniversary conference that "almost every great digital oak has a DARPA acorn at the bottom." Marine Lt. Gen. J. Amos said the US military will have to contend with a new era of guerrilla warfare in which an "arc of instability" encircles the globe equatorially. DARPA is hoping to develop weapons that would enable high-altitude patrolling of such regions by the United States. For example, DARPA leader T. Bussing envisions "an aircraft carrier in the sky" that can neutralize threats through countermeasures launched from anywhere in the continental United States that keep civilian casualties to a minimum. Amos expects missions by ground forces to consist of squads patrolling populous towns where distinction between friends and enemies is close to nonexistent, aided by situational awareness delivered via aerial platforms. Retired political scientist and author Chalmers Johnson is critical of DARPA's ambitious high-tech warfare visions, arguing that it is making the country less secure and driving it toward bankruptcy. "We spend billions of dollars to develop and procure innovative solutions ... but at the end of the day, it's still not possible for us to completely defeat these very basic technologies and approaches our adversaries are choosing," noted Deputy Secretary of Defense G. England at the DARPA conference. "And of course there's a huge cost disadvantage, probably a million to one between our outlays and what an IED builder spends on readily available parts." DARPA and Pentagon officials said at the conference that the United States will need to spend $1 million for every dollar spent by enemy guerrillas. "We are like a lion up against bees that are very effective whenever they swarm," said DARPA's D. Newman.

Digital Detectives Discern Photoshop Fakery
Christian Science Monitor (08/29/07) P. 13; C. Gaylord

Image-manipulation software has become increasingly easy to use and exponentially more difficult to detect, but H. Farid, a computer science professor at Dartmouth and head of the college's Image Science Group, has developed computer algorithms that can test photos to see if they are fakes by finding the tiny hidden flaws. "There's no way to push a button and tell if it's real, but there are tests we can run that allow us to be pretty sure if it's a fake," Farid says. Some of the techniques teach a computer to identify subtle imperfections that untrained humans have difficulty spotting, such as inconsistencies in the physics and geometry of the image. For example, the vanishing points may not match, or the shadows cast from two or more objects may contradict each other. While some of the tests seem simple, others are quite complicated. One of the tests checks the reflection of light in people's eyes to traingulate the location of the flash camera that took the picture. If the analysis shows that the camera was in multiple places, the photo is a fake. While a significant amount of image manipulation is done by tabloid media, fake photos are problematic for the legal system, and this is where Farid's software will be put to good use. Farid has already testified in more than two dozen court cases as to whether photographs were altered. He says that so far most accusations of fraud turn out to be unfounded.

Statistics Professor Says Databases Must Balance Privacy, Utility
Carnegie Mellon News (08/30/07), J. Potts

Carnegie Mellon University statistics professor G. Duncan says that organizations with large databases such as the US Census Bureau, which collects tremendous amounts of personal information, need to find ways to protect individuals' privacy while making the data available to researchers. Duncan believes that traditional methods of "de-identifying" records such as removing Social Security numbers and birth dates do not adequately protect sensitive information because if someone knows enough about the data they could use other characteristics to identify individuals. Unfortunately, the information that can be used to re-identify records is often the information that is most useful to the researchers. "The question is, 'How can data be made useful for research purposes without compromising the confidentiality of those who provided the data?'" Duncan asks. Possible solutions include establishing administrative procedures that restrict data access to approved personnel, implementing restrictions on the use of information, and developing statistical methods that de-identify records so that users cannot readily reconstruct personal identities but researchers can still view the required information. "Achieving 'adequate' privacy will require engineering innovation, managerial commitment, information cooperation of data subjects, and social controls," Duncan wrote in a commentary published in the journal Science.

Louisiana Tech Researchers Work on Cyber-Attack Defense
Associated Press (08/26/07)

Louisiana Tech University's new Center for Secure Cyberspace (CSC) is developing new technologies for use by the military and the private sector to protect electronic networks and wireless communications. CSC director Vir Phoha says the center has eight computer science researchers, four from Louisiana Tech and four from Louisiana State University. Tech vice president of research and development L. Guice says Air Force researchers at Barksdale Air Force Base will also contribute to the research efforts. Recently, the Air Force started setting up a cyberspace command at Barksdale, which could lead to a variety of cyberspace-related research projects. The CSC has been operating since June, and Phoha says that previous research by CSC computer scientists has lead to published cyber protection research on topics including advanced grid computing, how to find malicious code online, and how to detect clogged computers before access is denied. Phoha says a major area of research will involve sensor networks that could aid the military on the battlefield, including more advanced computer grids that could detect a terrorist suspect in Iraq, for example. The research is made possible by the Louisiana Optical Network Initiative, a fiber-optics network that connects supercomputers at the state's major research universities.

How Close Is World War 3.0?
Network World (08/22/07), C. D. Marsan

A series of coordinated, politically motivated cyberattacks against the Estonian government are provoking anxiety among American IT and network professionals about further incidents and what strategies should be followed to prepare for similar cyber-assaults on commercial networks. "As we move more critical infrastructure to the Internet and we depend on it more and more for communications, the threat [of cyberwar] is real," says Arbor Networks security researcher J. Nazario. The success of the Estonian attacks and the media attention they attracted could encourage other people or groups with an axe to grind to launch similar exploits, warn experts. Most security experts say the Estonian incident was not an instance of all-out cyber warfare because there is no evidence that a government was behind the attacks. E. Spafford, executive director of Purdue University's Center for Education and Research in Information Assurance and Security, says authentic cyberwar would be an attempt by a country to impose its will on another, and network attacks would probably function as a complement to physical assaults. Columbia University professor S. Bellovin believes cyberterrorists or hactivists are more likely to attack individual commercial or government targets than wage an all-out cyberwar. Security experts concur that the Estonian incident should serve as a wake-up call for CIOs, who have generally ignored the threat of politically motivated attacks in favor of profit-oriented ones. ISPs, banks, and oil and electric companies are considered ripe targets for politically motivated cyberattacks. Spafford says it is important for US companies to realize that small groups of hactivists can cause considerable damage, as the Estonian attack demonstrates. The incident also shows that the strategy of acknowledging the problem and seeking help from ISPs and international governments can be successful.

FBI Launches Cybersecurity Project
Government Computer News (08/20/07), W. Dizard

The National Center for Supercomputer Applications at the University of Illinois at Urbana-Champaign will host the FBI's National Center for Digital Intrusion Response, a new law enforcement cybersecurity research center. The FBI will provide $3 million to support the first two years of the program, which represents an expansion of the FBI's existing work with the university. "This effort will benefit the scientists, engineers and other researchers who use cyber-resources at NCSA and other federal centers by protecting the cyberinfrastructure they rely on," says NCSA director T. Dunning. University IT security scholars will work with FBI cybersecurity specialists to understand what capabilities are necessary to detect and investigate cyberattacks, develop new tools, and ensure FBI agents in the field can use the tools effectively. The bureau says NCSA was chosen because it has 22 years of experience protecting high-performance computers from cyber attacks, including developing software for data analysis, visualization, collaboration, and communication. Expanding the bureau's work with the university is a reflection on the changing patterns of crime and national security threats. "While cyberattacks were once considered a specialized niche in law enforcement, today there are digital aspects to many crimes and national security threats; all investigators must be able to pursue criminals operating in cyberspace," the FBI says.