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

Δελτίο 51
15 Δεκέμβρη 2006

Panel Backs Guideline Favoring Voting-Machine Verification
Washington Post (12/06/06) P. A9; C. Barr

After failing earlier this week to pass a measure recommending that e-voting machines be required to allow audits independent of their software, the Technical Guidelines Development Committee (TGDC) has unanimously agreed upon a new version of the resolution, which grandfathers in existing systems but states that the "next generation" of e-voting machines should have such independent audit capacities. Electionline.org director D. Chapin says, "This seems to mark the end of an era" for e-voting without a paper trail, but many point out that there is no money left to be spent on new election systems. No timeline was given by the TGDC, which advises the US Election Assistance Commission (EAC), but many in Congress and local politicians have pledged to begin exploring options to carry out the recommended reforms. Virginia General Assembly Delegate T. Hugo said that "the committee recommendations...will really make people stand up and pay attention" to the changes that must take place. The report also stated that all disabled voters should be able to verify their votes, and that election officials and voting machine manufacturers should be charged with ensuring security measures. The National Institute of Standards and Technology's M. Newman said the panel has until July to create a set of standards to submit to the EAC.

Spam Doubles, Finding New Ways to Deliver Itself
New York Times (12/06/06) P. A1; B. Stone

After being successfully foiled by anti-spam software to the point that they were no longer a major concern at the beginning of the year, spammers have found new techniques of flooding mailboxes and consuming bandwidth. Spam filtering firm Ironport claims that spam volumes worldwide have doubled from last year, and that junk email now makes up over 90% of e-mails sent. By embedding text in images, spammers found a loophole in spam-blocking technology, which scans traditional email text to detect telltale signs of spam. The use of botnets now makes blacklists unreliable as well as allows spammers to send more messages without being charged for generating the data traffic. Ironport's P. Peterson admits that, "The bad guys are simply outrunning most of the technology out there today." By adding speckles or flowery patterns to images where text was imbedded, spammers even confused programs designed to detect text in images. They have also developed a way to change just a few pixels in each email sent out, creating a unique "fingerprint" for each, so programs that identify a message as spam and eliminate all copies no longer work. Linking violators to incriminating Web sites has gotten more complicated, as the "pump and dump" technique is now quite popular; where spammers purchase cheap stock in an obscure firm, send out email advertising the stock, and sell when enough unsuspecting people buy the stock. Today's spammers operate out of Russia, Eastern Europe and Asia, according to expert, making them immune to strict US anti-spam legislation.

Carnegie Mellon Researchers Uncover Online Auction Fraud
AScribe Newswire (12/05/06)

By analyzing the publicly accessible transaction histories of online auction sites, Carnegie Mellon University researchers have been able to identify suspicious behavior and associations between users, using data mining techniques. These fraudsters, such as those who take money for the sale of an item and never mail it, accounted for 97,000 complaints passed along to law enforcement by the federal Internet Crime Complain Center, and can now be located and purged from auction sites. By identifying accomplices, the emergence of new fraudsters can be prevented as well. The system, known as Network Detection via Propagation of Beliefs (NetProbe), gives a numerical rating of trustworthiness that cannot be manipulated the way reputation systems used by the auction sites can be. Accomplices, who do not commit fraud directly, use their favorable reputation to boost the feedback ratings of fraudsters, but this can be detected using a graph of transactions, where users are represented as nodes and transactions as lines connecting the nodes. Researchers found that in such a graph the transactions completed between accomplices and fraudsters shows a "bipartite core," meaning one group has a great deal of transactions with another but none within its own group; the accomplice group also deals with honest users but mostly with fraudsters. This technique has been tested on massive sets of data and is currently being used to examine about a million e-Bay transactions.

Civil Libertarians Protest Privacy Policy
Washington Post (12/06/06) P. A11; Nakashima, Ellen

New privacy regulations, and the board created to oversee them, are drawing criticism from various civil liberties groups, who have cited the protections guaranteed by the Privacy Act of 1974. Electronic Privacy Information Center executive director M. Rotenberg points out that "the absence of transparency, the absence of oversight, and the inability for individuals to know what information about them is being collected by the federal government." The guidelines, drafted by the Office of the Director of National Intelligence, state that information obtained on "US persons" be done so legally, and be shared only if it is relevant to terrorism or law enforcement; however, the guidelines do not require that those affected be notified. Markle Foundation privacy task force member J. Dempsey says the privacy regulations also fail to address data-collection standards or establish appropriate methods to deal with those who have been mistakenly targeted. The privacy board, which has only five members, is part of the executive branch and does not have the power of subpoena, causing civil libertarians to call for the establishment of a more independent, capable body. ACLU legislative director C. Fredrickson said the board has no power to alter policy on some of the most pertinent issues. Broader oversight of the government's data-mining policies and terrorism surveillance programs have been promised by Democrats poised to take over Congress next year.

Q&A: Responsible Disclosure of Vendor Flaws and What It Means
Computerworld (12/04/06), J. Vijayan

Publicly disclosing vulnerabilities in software products is about increasing the pressure on software vendors to improve the security of their applications, according to vulnerability researcher H. Moore in an interview with Computerworld. Moore, who has been involved with the independent group of security researchers behind the controversial Metasploit Project, says the various initiatives he has undertaken were meant to raise awareness of flaws in software and the potential impact of the vulnerabilities on an organization. Though Moore and other independent security researchers have come under fire for making it easier for bad guys to exploit software vulnerabilities, he says his critics are not facing reality. He maintains that hackers exploiting the most problematic flaws are often caught before word of the vulne-

rability goes public. And he views responsible vulnerability disclosure as a flawed approach to software security because not disclosing flaws publicly does not necessarily mean software users will be safer. Moore believes his security efforts, from posting vulnerability information to releasing the Metasploit Framework tools, have largely been a success.

Health Hazard: Computers Spilling Your History
New York Times (12/03/06) P. 3-1; M. Freudenheim; R. Pear

While health insurance companies, tech companies, and the US government are all pushing to computerize the health records of Americans in order to improve the ability of the medical profession to share information in the name of making valuable advances, many people are wary of the potential risks of making such information widely available. A Markle survey found that 56% of respondents were very concerned about abuse by employers, though nearly all respondents were eager to experience the benefits Internet technology could bring to health care. Some employees fear they could lose their job due to expensive medical conditions, as such instances have been found to occur. In many cases, employees have the decision whether or not to submit their information to be put into an electronic database, but some companies are even offering small sums of money for those willing to cooperate. While most large companies claim that personnel professionals do not have access to medical information of employees, many suspect that there are companies where those in charge of insurance claims also handle hiring and firing decisions. Unfortunately, charges are rarely brought against those who illegally access medical records. Due to fears of lawsuits resulting from sharing data, American primary-care physicians make use of electronic health care information systems far less than their counterparts in England or in the Netherlands, according to the journal Health Affairs. The new Democratic Congress has already pledged to address this issue of privacy once it takes power next year, according to Rep. E. Markey (Dem.-Mich.).

Open-Source Spying
New York Times Magazine (12/03/06) P. 54; C. Thompson

There is a glut of chatter for intelligence agencies to sift through to find evidence of terrorist plots or other kinds of criminal activity, and it is hoped that wikis or blogs might help ease the burden and revolutionize analysis. The idea was spawned from an essay written by C. Andrus of the CIA's Center for Mission Innovation, which posited that it is the explosion of self-publishing in which the real power of the Internet resides; Andrus noted that blogs and wikis are self-organizing, and theorized that if agents or analysts posted blogs and wikis on the Intelink network, then mob intelligence would ensue and facilitate a democratic process of information sharing. Perhaps even more significantly, the blogs and wikis could substantially enhance Intelink's search engines. With such an approach, clues of a terrorist plot such as the one responsible for the 9/11 bombing would inexorably come together and gain authority in the intelligence community, Andrus suggested. A wiki's usefulness to intelligence analysis is being tested with Intellipedia, a prototype wiki for intelligence employees; agents are encouraged to add to the wiki's content, which consists of hundreds of articles from nonclassified documents. T. Fingar with the office of the director of national intelligence (DNI) admits that Intellipedia will not eliminate the likelihood of false or erroneous reportage, but he thinks a sufficient number of contributing analysts will catch major mistakes. Meanwhile, DNI CIO D. Meyerrose directed the creation of a test blog for intelligence collection. New York University professor C. Shirky says the success of "social software" for intelligence agencies depends on convincing thousands of analysts to start blogging and producing wikis, and key to this will be shifting agents' secretive mindset to one that is more open to sharing.

But there are concerns that such an approach could expose potentially dangerous information to the wrong people.

Tomorrow's Security Today
InformationWeek (12/04/06)No. 1117, P. 45; L. Greenemeier

Under development today are future security technologies that stand out in terms of their proactivity. The linkage between physical and IT security technologies is a central component of video surveillance, and upcoming innovations in this domain include IBM's Smart Surveillance middleware, which embeds analytical capabilities into camera, chemical-sensor, radar, and audio surveillance systems for the detection of suspicious activity; 3VR Security CEO S. Russell says the market for recording and managing video surveillance was revolutionized by the storage of digital video on hard drives. J. Platon with Cisco Security Solutions says the next few years will see the availability of technology that can match images of employees and visitors with video footage of people walking through a business' front door, once facial-recognition software improves. Standards for protecting systems and data from outside attacks and physical theft are under development by the Trusted Computing Group: Examples include the Trusted Network Connect standards for network access control technology and the Trusted Platform Module for the special storage of user credentials off the hard drive. Wave Systems CEO S. Sprague predicts that within a decade, "You will authenticate the human being to the machine, and the machine will authenticate you to the network." Advanced fingerprint authentication solutions from the likes of Nanoident Technologies are also on the horizon. The biometric sensors Nanoident makes can reportedly scan prints, tissue structure, and hemoglobin levels, while CEO K. Schroeter says the wide implementation of fingerprint authentication technology requires an upgrade in accuracy. Around the close of the decade, companies will be capable of ascertaining whether criminals can blend together seemingly harmless pieces of information about clients, employees, and partners to access sensitive data through innovations pioneered by groups such as the Palo Alto Research Center's security and privacy research unit, which is working on privacy monitoring software with a data inference assessment application.

Big Shift Seen in Voting Methods With Turn Back to a Paper Trail
New York Times (12/08/06) P. A1; I. Urbina; C. Drew

Federal election officials and legislators have indicated that major changes will most likely be seen in the way ballots are cast and counted by the 2008 elections, including the elimination of voting machines without a paper trail. New federal guidelines issued this week and legislation expected to pass next year are causing voting districts to either retrofit touch-screen machines with printers or otherwise scrap them all together and implement optical scan machines. Paperless, touch-screen voting machines were used by about 30% of voters in the 2006 mid-term elections, but scientists and politicians have become increasingly concerned about the security and reliability of those machines. However, federal Election Assistance Commission Chairman P. Degregorio points out that counties that used paper trails ran into problems of their own, urging officials to think their decision through so that old flaws are not simply replaced with new ones. Legislation Congress is expected to pass next year will allocate $150 million to fund the necessary changes in local voting procedures, but some claim this would not be enough money. As part of the new election regulations, vote counting software code likely will have to be made available so it can be checked for vulnerabilities, although the manufacturers claim that doing so will only help hackers. Voting machines will also be subjected to new federal tests prior to elections. VoteTrustUSA's W. Stewart says, "We're confi-

dent that the accuracy and integrity of voting is going to take some big steps forward with the legislation in Congress right now. But our big concern is to avoid replacing old problems with new ones."

Guest Lecturer Focuses on Cybersecurity Threats
UDaily (University of Delaware) (12/07/06), B. Hutchinson

ACM fellow E. Spafford on Wednesday spoke at the University of Delaware concerning the precarious state of cybersecurity and the dangers to come if safety measures are not improved. Spafford, Purdue University professor of computer science and executive director for its Center for Education and Research in Information Assurance and Security, made it clear that cybersecurity is facing a crisis with "overwhelming vulnerabilities in most commonly used software applications, and well over 130,000 known viruses and worms." Mentioning that cybercrime in general has becoming more sophisticated, "because we have not done a very good job of protecting ourselves," Spafford identified botware as the newest and largest threat. He stated that "Detection is doomed and the problem is getting worse...two out of 40 individuals is a victim of identity theft, and [only] one out of every 10 email messages is valid." The apathy toward the idea that "we're not simply users, we're victims" is Spafford's biggest concern, and he attributed blame to a lack of ownership of the Internet, the increasing abilities of hackers, and the lack of funding for math and computer science education in American public schools. He claimed that clinging to yesterday's security measures, firewalls, and virus-protections software is "insanity."

DHS Passenger Scoring Illegal?
Wired News (12/07/06), R. Singel

Privacy advocates charge that the Dept. of Homeland Security's Automated Targeting System (ATS), which assigns terrorism scores to people traveling in and out of the United States, is a violation of the limits that have been placed on the department by federal lawmakers. Pointing to a provision in the 2007 Homeland Security funding bill, Identity Project members E. Hasbrouck and James Harrison wrote, "By cloaking this prohibited action in a border issue...the Department of Homeland Security directly and openly contravenes Congress' clear intent. A DHS spokesperson said the appropriations bill's language--which bars government agencies from using appropriations funding to "develop or test algorithms assigning risk to passengers whose names are not on government watch lists"--does not cover the ATS, which harvests passenger data from international flights and scores each passenger's risk based on watchlists, criminal databases, and other government systems. High scorers are targeted by Customs and Border Protection for extra screening at deplaning time, and the data and scores can be kept for 40 years, broadly shared, and be used for hiring decisions; in addition, travelers are not able to see or contest their scores. According to congressional testimony by DHS official P. Rosenzweig, the system had "encountered 4,801 positive matches for known or suspected terrorists," although it was not clear how many were correct matches. Critics who say the ATS program is illegal under the law include M. Rotenberg of the Electronic Privacy Information Center and J. Harper of the Cato Institute. DHS spokesman J. Agen argues that the appropriations bill's language refers specifically to a program called Secure Flight, a planned successor to the CAPPS II screening system, but Rotenberg and Harper disagree with that interpretation.

The Privacy Klatch
National Journal (12/02/06) Vol. 38, No. 48, P. 52; S. Harris

Nascent and current technologies that could be employed for the protection of civil liberties during data collection and analysis are the focus of "privacy workshops" sponsored by the Office of the Director of National Intelligence (DNI). "It was clearly an effort to reach outside of the intelligence community and reach outside of the classified environment," noted J. Dempsey of the Center for Democracy and Technology. A. Joel with the DNI's Civil Liberties and Privacy Office explained that participants recommended several technologies, such as tools for comparing multiple databases without sharing data, and data-misuse prevention technologies such as devices that generate "audit logs." Certain privacy proponents and technology experts, including some very vocal critics of the Bush administration, were not invited to the workshops, while attendees said arguments over policy were avoided. "I think the overall aim is to look at increasing the body of knowledge [on privacy protection], to further technical research within the DNI," said Factiva director of government services T. Hall. It is no coincidence that the DNI's office is taking the reins of research that was originally conducted under the auspices of the Defense Department's now-defunct Total Information Awareness (TIA) project, with certain TIA component programs folded into the DNI and included in the Tangram program. The Tangram manager pledged that civil liberties officials would be consulted prior to the deployment of the new program. The advice of privacy workshop participants will be used by DNI officials to establish a research agenda for guaranteeing privacy in new counter-terrorism solutions and to bolster their cognizance of the cutting edge.

Traveler Data Program Defied Ban, Critics Say
Washington Post (12/09/06) P. A2; S. Spencer; E. Nakashima

The Department of Homeland Security's Automated Targeting System (ATS) has come under fire from key members of Congress and privacy advocates who claim it was developed and carried out without proper disclosure, and thus violates a congressional funding ban. The ATS, which was stepped up after 9/11 to create risk assessments of travelers crossing U.S. borders that are retained for up to 40 years, was first disclosed in some detail in a November 2 Federal Register notice, which DHS claims was an attempt to be more clear about what they planned to do. Travelers do not have access to their risk assessments, and would have to file Freedom of Information Act requests just to see the records on which the assessments are based. The Center for Democracy and Technology claims that the ATS is in violation of the 1974 Privacy Act, noting that information on travelers is shared between agencies with no notice given to the public. The DHS has stated that the funding ban only applies to programs stemming from its failed 2004 attempt to assign risk ratings to passengers on domestic flights using commercial databases, not preexisting programs such as ATS, and stands by its use of data to "detect anomalies and 'red flags.'" "Otherwise, why are we collecting the data?" asked Homeland Security Secretary Michael Chertoff. Recent DHS correspondence has explained that ATS uses data-mining and computer algorithms to search for "potential matches" of travelers with "connections to terrorist risk factors."

Researchers Crafting Intelligent, Scaleable WLAN Defense Through DARPA
Network World (12/07/06), J. Cox

A research project at Dartmouth College has been developing a system of algorithms and software architecture that analyzes WLAN traffic to detect and react to attacks. Though intrusion-detection systems (IDS) are currently available, Project MAP (measure analyze and protect), sponsored by the Defense Advanced Research Projects Agency (DARPA) and Aruba Networks, is able to monitor the interaction of thousands of access points and clients as well

as the measurement data it creates itself. Aruba security researcher J. Wright says, "Attackers are using evasion techniques, and these are not being addressed by today's [IDS] products." The project must achieve scalability so RF sensors can perpetually track, gather, and combine large amounts of real-time information concerning a site's radio environment. Using many Aruba RF sniffers, MAP software combines that data to form an accurate image of what is going on in the air, and searches for evidence of attacks. Where other IDS systems monitor every frame to check for matches with attack signatures, MAP looks at higher-level statistics to detect patterns indicating malicious activity. Ideally, the system would develop into a dynamic WLAN security application able to watch for and adapt to attacks that are constantly being altered.

Informatics Scientists' 'Active Cookies' Put Bite on Cyber Crooks
Indiana University (12/07/06)

Active cookies could be a solution to fighting identity theft and other kinds of cyber attacks, according to researchers at Indiana University School of Informatics and RSA Laboratories in Massachusetts. Active cookies prevent hackers from interfering with the Domain Name System translation in an attempt to steal the coded pieces of information stored on a user's computer. "The reason is simple: Active cookies use one step that requires no translation," explains informatics associate professor M. Jakobsson. Attackers can steal regular cookies stored on a computer and gain access to accounts with hopes of obtaining personal information that will allow them to impersonate the users, but they cannot take advantage of active cookies unless they steal the personal computer where the coded pieces of information are stored. A bank would be able to place active cookies on the home and work computers of a customer to protect the individual from phishing attacks. "And you can still log in if you travel, you might have to provide some additional identifying information then, or your bank can compare your login location with the location of your last ATM withdrawal," Jakobsson says. Jakobsson and research partners Sid Stamm, a computer science doctoral student at IU, and A. Juels of RSA will present their work at the 14th Annual Network & Distributed System Security Symposium in San Diego in February.

Spam Choking the Internet Again
New Scientist (12/08/06)

Two years ago Microsoft Chairman B. Gates predicted that the spam problem would be under control by 2006. However, today, spam is nowhere near under control. Spam is still a worldwide issue with IronPort Systems reporting that global spam volumes have gone up from 31 billion messages a day in October 2005 to 61 billion messages a day in October 2006. A recent study by Postini found that spam makes up 91% of all email messages. The reason for the massive increase is that spammers have become sophisticated and now use botnet computers to send out messages. One million botnets can send 50,000 or more spam messages at once, according to Postini. "This dramatic rise in spam attacks on corporate networks has the Internet under a state of siege," says D. Druker at Postini. "Spammers are increasingly aggressive and sophisticated in their techniques, and protection from spam has become a front-burner issue again." Spammers are often motivated by financial gain--they can profit by directing users to phishing sites in an effort to steal financial data or passwords. Meanwhile, image spam is increasingly being used because it is often undetected by filtering systems. Image spam made up 25% of all spam this past October.

Better, Faster, More Secure

Queue (01/07) Vol. 4, No. 10, B. Carpenter

IBM Distinguished Engineer and chairman of the Internet Engineering Task Force (IETF) Brian Carpenter writes that the lack of centralized Internet control is one of the reasons why it is difficult to predict future technology trends. He can recall past forecasts he made, predicting computer-supported collaborative work as a killer app, the integration and domination of Internet and IPX, and a devaluing of transaction processing--none of which have come to pass. Carpenter figures that the online security model must shift from a defensive posture (firewalls, filters, and virtual private networks) to one that stresses authentication, authorization, and accounting. Within this area lies the challenges of defining, authenticating, and maintaining the privacy of identity; creating trust relationships between arbitrary sets of parties; agreeing on cryptographic keys among such parties; shielding packet origins against spoofing at line speed; and continuing to get messages from unknown parties without receiving undesirable messages. The quality of service (QoS) of packet delivery remains challenging: Approaches Carpenter recognizes include competent design and management of a network, bandwidth overprovision, traffic engineering, and differentiated services, all of which much be seamlessly integrated by service providers. Fourteen years ago, two major Internet problems were cited in a request for comments by the IETF steering group--the depletion of IP address space, which is being addressed by IPv6 implementation, and the routing table boom, which is still unresolved. Carpenter lists the fundamental principles upon which the International Telecommunications Union's Next Generation Networks (NGN) effort is founded, which include MultiProtocol Label Switching (MPLS)-facilitated IP packet-based transport, QoS enablement, embedded service-related functions, user access to rival service providers, and generalized mobility. The author reports that the standardization of NGN around these principles is moving forward.