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

Δελτίο 95
4 Νοέμβρη 2007

From Casinos to Counterterrorism
Washington Post (10/22/07) P. A1; E. Nakashima

Las Vegas, with its wide adoption of data mining and surveillance, is being viewed by some privacy advocates as a template for future US security, with its emphasis on preventing terrorist attacks. Cameras in casinos--and sometimes facial recognition systems--monitor players and employees, while surveillance specialists analyze the input and run it against databases to uncover potentially suspicious activity. One program developed for the casino industry, Non-Obvious Relationship Awareness, uses link analysis to find evidence of collusion between gamblers and casino employees, and the program was successful enough to inspire the Dept. of Homeland Security to look into it as a tool for uncovering terror networks. Bets are also tracked via RFID-outfitted casino chips, and counter-terrorism and Homeland Security officials are investigating the embedding of RFID chips in various objects--passports and other IDs, for instance--for the purpose of tracking people and their communications that might lead to a terrorist network. Some say iris-scan technology will be suitable for use in gaming in a few years. Center for Democracy and Technology policy director J. Dempsey is particularly troubled that the use of such methods has spread to counter-terrorism. "Finding a terrorist is much harder than finding a card counter, and the consequences of being wrongly labeled a terrorist are much more severe than being excluded from a casino," he says. ACLU official B. Steinhardt is similarly concerned that the convergence of all these various technologies is giving rise to a "surveillance society."

What's Russian for 'Hacker'?
New York Times (10/21/07) P. WK1; C. Levy

Russia has become a major breeding ground for hackers who use their anonymity to inflict mayhem on the West, aided by the Russian government's apparent indifference to their activities. The roots of Russian hacktivism include the country's strong system of math and science education, generally poor job prospects for graduates of Russian technical institutions, and societal encouragement of rule-breaking as a form of resistance against the strictures and despotism of the Communist regime. This resulted in widespread corruption that has continued beyond the collapse of the Soviet Union, of which hacking is one manifestation. "There was always a great entrepreneurial spirit in Russia, but it has always been directed at things that not only help people, but also hurt people," notes Russian-American author G. Shteyngart. Most Russian hackers are driven by a desire to profit financially, and Russia has more scammers than the United States and China. Rough estimates place 28 million Internet users in Russia, versus 150 million in China and 210 million in America. Russian hackers are considered by VeriSign to be the worst type of hackers because of their links to organized crime outfits that embezzle money with stolen bank and credit card information. Russian Parliament member A. Likhachev claims the lack of criminal hacker cases in Russia is less a matter of indifference and more a matter of officials facing a learning curve in enforcement and prosecution against such activity.

To Maintain National Security, US Policies Should Continue to Promote Open Exchange of Research, National Academy of Sciences (10/18/07)

The US should make the open exchange of unclassified research a priority as it is essential to the science and technology research necessary for maintaining national and economic security, concludes a National Research Council report. "In the years following the Sept. 11 attacks, research institutions have established policies and procedures that address concerns about security," says council co-chair J. Gansler, vice president for research at the University of Maryland, College Park. "However, both the security and scientific communities agree that losing our leading edge in science and technology is one of the greatest threats to national security. Unnecessary or ill-conceived restrictions could jeopardize the scientific and technical progress that our nation depends upon." While the National Security Decision Directive 189 was enacted to ensure research remains open to the public and foreign contributors, recent government policies and practices have essentially reversed the directive. What is now needed is for the government to establish a standing entity, a Science and Security Commission, to review policies regarding the exchange of information and participation of foreign scientists. The report suggests that the commission include representatives from academic research institutions and national security agencies, and should be co-chaired by the national security adviser and the director of the White House Office of Science and Technology Policy. "The US security and research communities need to work together to weigh the latest information about potential threats and ensure the continuation of scientific research that could help mitigate them," says council co-chair and president of Lehigh University A. Gast.

Research Shows Image-Based Threat on the Rise
Dark Reading (10/18/07), K. Higgins

New research at Purdue University shows that steganography may now be a more significant threat than previously thought. Once considered to be too complex and conspicuous, some forensics experts now believe that steganography is being used more frequently, particularly in child pornography and identity theft trafficking. It is estimated that there are about 800 steganography tools available online, many for free and with user-friendly interfaces that allow for point-and-click use. Previous studies that searched for hidden steganographic messages produced few results, giving credence to the belief that steganography is not a mainstream threat. However, the new Purdue study has found evidence of steganography tools on convicted criminals' computers. Even if a criminal removes a steganography program it leaves behind "footprints" so the researchers can find evidence that the tools were once there. Previously, Purdue researchers looked for images with embedded steganography images online, but professor James Goldman realized that it would be easier to try to prove whether criminals were using steganography tools than to find the images. "Never mind finding the evidence of what they are sharing or the secret message, but just proving they use it," Goldman says. "This is the first time this has been done, I think." Goldman is working to discover which steganography tools are the most popular so researchers can do more "granular" work on popular tools and find more information on how they are being used.

Air Force's Future Lies in Cyberspace
Washington Times (10/19/07) P. A9; S. Waterman

The Air Force's recent declarations that cyberspace is a "war-fighting domain" have raised questions about US military policy and doctrine. Air Force Lt. Gen. R. Elder, who is in charge of the Air Force's daily cyberspace operations, says the speed, range, and flexibility of the Air Force relies entirely on the military's cyber-dominance. The Air Force is currently establishing a Cyberspace Command to match its space and air command, but Elder and other officials deny that the Air Force is making a turf grab. Elder says that cyberspace is similar to maritime and air domains in that each are used for commerce and daily life, but are potential vectors of military action by or against the United States. The legal framework and authorities on activities in cyberspace are hazy, and the full implications of managing cyberspace as a war-fighting domain are still unknown. Elder says the Air Force is working with civilian agencies, law enforcement, and the Dept. of Homeland Security to fill the gaps between civilian and military authority in cyberspace. Elder says that although some think that laws on cyberspace might need to be changed, no consensus has been reached. Some Air Force officials believe current US military policy is too timid. "Legislation, policies, and international law are lagging the technology," says L. Kass, senior advisor to US Air Force Chief of Staff Gen. T. Moseley. "The United States is late to the fight."

House Panel Chief Demands Details of Cybersecurity Plan
Baltimore Sun (10/24/07) P. 1A; S. Gorman

House Homeland Security Committee Chairman Rep. B. Thompson (D-Miss.) on Tuesday called upon the Bush administration to postpone the rollout of its cybersecurity initiative so that a congressional evaluation of the plan's legality could be performed. The program seeks to leverage the surveillance resources of the National Security Agency and other entities to shield government and private communications networks from hackers and terrorists. Thompson submitted a letter to Homeland Security Secretary M. Chertoff in which he demanded that a briefing on the plan's details be sent to his committee, and that "significant questions" concerning the program's "centralization of power" should be addressed prior to launch. Thompson said issues of privacy and domestic surveillance would be of particular interest to his committee, given the NSA's and similar agencies' involvement in the plan. "What's the legal framework about which civil rights and civil liberties, as well as constitutional issues, will be protected?" Thompson queried. Current and former government officials familiar with the program say the plan calls for a seven-year, multi-billion-dollar initiative with up to 1,000 or more employees from Homeland Security and other agencies. The plan's first phase would involve the establishment of a system to guard government networks from cyberattacks, while a later phase would augment the security of private networks that control communications, nuclear power plants, electric-power grids, and other vital systems. Thompson was upset that the administration kept the plan under wraps and said further silence on the matter would prompt him to consider issuing a congressional subpoena.

UD Computer Security Campaigns Win Awards
University of Delaware (10/23/07), J. Rhodes

The University of Delaware was awarded two major honors for its efforts to promote computer security at the 35th annual ACM Special Interest Group on University and College Computing Services Conference (ACM-SIGUCCS), held Oct. 7-10 in Orlando, Fla. Its "National Cybersecurity Awareness Month" received the Award of Excellence in the General Service Campaign category, which includes publications that boost the visibility of computing efforts at institutions of higher learning. The campaign included a weekly video tip, each 65-90 seconds long, that revolved around the central theme "Protect Your Computer." The purpose of the videos "was to raise public awareness and to lead people to information to help them protect themselves, their information, and their computers," says R. Gordon, a project participant and member of UD's IT-User Services. The videos were accompanied by promotional articles in UD's daily paper and a calendar of cybersecurity awareness activities posted on the school's IT-Help Center Web site. Also getting recognition at the conference was UD's "Connecting Your Computer to UDelNet: Your UDelNet ID and Security," which won an Award of Excellence in the Electronic How-to Guides category. "Last year, these episodes of connecting videos were by far the most downloaded and viewed of the 'Consulting on Demand' series," says L. Larraga, also of IT-User Services. "We were pleased to have its success affirmed by our academic community peers."

Scientists Draw on New Technology to Improve Password Protection
Newcastle University (10/24/07)

Newcastle University researchers are developing a new password protection system that uses pictures instead of letters and numbers, creating what they believe is a simpler, safer, and more memorable password system. The technology can currently be used on devices such as iPhones, BlackBerrys, and smart phones, but could also be adapted to help people with language difficulties such as dyslexia. Newcastle University lecturer J. Yan and PhD student P. Dunphy say their work improves upon the emerging graphical password technology called Draw a Secret (DAS). DAS allows users to draw an image as a substitute for a password, which is then encoded as an ordered sequence of cells. The researchers superimposed a background over the DAS grid to create the Background Draw a Secret system (BDAS). BDAS helps users remember where they started the drawing and creates graphical passwords that have more stroke counts, making passwords that are less predictable, longer, and more complex. During a trial of the BDAS system users were asked to select a background and draw a password image. One week later, the participants were asked to re-create the image and were able to do so with 95 percent success within three attempts. "The recalled BDAS passwords were, on average, more complicated than their DAS counterparts by more than 10 bits," says Yan. "This means that the memorable BDAS passwords improved security by a factor of more than 1024."

'Half-Quantum' Cryptography Promises Total Security
New Scientist (10/21/07), P. Marks

Many cryptographers believed that the only way to achieve complete security when transmitting information was to use quantum cryptography to share the key used for encryption. However, researchers say they can achieve the same level of security even if one party stays in the world of classical physics. In conventional quantum cryptography, a sender, dubbed Alice, generates a string of 0s and 1s and encodes them using a photon polarized in either the computational "basis" in which 0 and 1 are represented by vertical and horizontal polarizations, or in diagonal bases in which 1 and 0 are represented by 45 degree and negative 45 degree polarizations. When the photons arrive at their destination, the receiver, dubbed Bob, chooses either the computational or diagonal bases to measure each one, telling Alice which he has chosen. If the chosen basis is wrong, Alice tells Bob to discard that bit. The bits that are guessed correctly form the secret key. If an eavesdropper intercepts any photons, the stream is interrupted and Bob's ability to read a number of the photons he might have read correctly is destroyed. The increase in unreadable photons tells Bob the communication channel has been compromised. Researchers at the Israel Institute of Technology in Haifa and the University of Montreal have demonstrated that only Alice needs to be quantum-equipped. Alice encodes the bits as usual, though Bob can only use the computational basis. Bob randomly measures some of the received photons and returns the rest to Alice untouched. The bits read in the computational basis form the key. The system is still secure because anyone eavesdropping does not know which photons will be returned to Alice unmeasured.

Identity Theft: Costs More, Tech Less
Network Computing (10/23/07), T. Claburn

A study by Utica College's Center for Identity Management and Information Protection (CIMIP) revealed that the median actual dollar loss for victims of identity theft is $31,356, a much higher figure than suggested by past studies. However, earlier studies primarily concentrated on consumer losses, whereas Utica's study reviewed 517 cases investigated by the US Secret Service, which tend to be major incidents, not minor scams. Indeed, the CIMIP study is the first to review the Secret Services' closed case files, and as such aims to provide empirical data. The report proved that companies as well as individuals are affected by identity theft. The study also discovered that the Internet is not always an essential tool for identity thieves. Of the 517 cases reviewed, 102 cases involved Internet use and 106 involved non-technological means, such as mail rerouting. In other instances, criminals used mail theft to access sensitive information and then used Internet-related tools to create fake documents. Another unanticipated finding was that in the 274 cases with identifiable points of compromise, businesses were the starting point for half of the breaches. Moreover, one-third of the identity theft cases reviewed implicated insiders. Finally, the study's results challenged the belief that most identity thieves are white males, as roughly 50% of the offenders were black and roughly 40% were white. CIMIP works with corporate, government, and academic institutions to research identity management, information sharing, and data protection, including the Carnegie Mellon University Software Engineering Institute, Indiana University's Center for Applied Cybersecurity Research, and Syracuse University's CASE Center.

Password-Cracking Chip Causes Security Concerns
New Scientist (10/24/07), A. Brandt

Russia's Elcomsoft has filed a US patent application for a technique for cracking computer passwords using inexpensive off-the-shelf computer graphics hardware. Using an inexpensive graphics card, Elcomsoft was able to increase its password cracking speed by a factor of 25, says Elcomsoft's V. Katalov. The most difficult passwords, such as those used to log onto a Windows Vista computer, would normally take months of continuous computer processing using a normal central processing unit. However, Katalov says they can be cracked in as little as three to five days by using a graphics processing unit. He says less complex passwords can be cracked in a few minutes instead of hours or days. The speed increase comes from how a GPU processes information. Password cracking is an effective way to access information on a computer, but is generally ineffective at accessing online banking services since their Web sites often require multiple passwords and shut down after several incorrect attempts. Cryptography Research's B. Jun says the technique is an impressive achievement that required elegant, intelligent design, and while the ability to crack passwords using GPUs is concerning, it is not a cause for panic. Advancements in cryptographic keys and the growing trend of encrypting entire hard drives is making accessing sensitive data more difficult. "Should I throw away my Web server and run for the hills?" asks Jun. "I don't think so."

Workforce Issues Complicate Planning for Cyberattacks
GovExec.com (10/25/07), G. Nagesh

The Homeland Security Department is struggling to recruit and retain expert cybersecurity officials, which is impairing the department's ability to carry out certain tasks. More specifically, the workforce dilemma has slowed the department's development of a far-reaching cyberattack recovery plan, according to G. Wilshusen, director of information technology at the

Government Accountability Office. In 2006, DHS outlined a strategy for how corporations and the government could recuperate from an Internet-disrupting cyberattack. DHS delegated response coordination to the National Communications System, as well as protection of security infrastructure and hardware. The National Cyber Security Division would be in charge of securing the integrity of the data under attack and software applications. However, to date, "there is no public-private plan for recovery and there is no date by which such a plan must exist," says Wilshusen. Multiple factors have hampered DHS from preparing a complete strategy, including the agency's organizational and leadership disarray. Wilshusen attributes DHS' struggle to retain the best talent to "the nature of cybersecurity work," which typically involves long hours of fast-paced and rigorous work. Other reasons for the plan's delay include cyberattacks' constantly evolving nature as well as the Internet's extensive intercomnectivity.

Space Station: Internal NASA Reports Explain Origins of June Computer Crisis
IEEE Spectrum (10/07), J. Oberg

On June 13, the International Space Station's functions were crippled by the faulty design, construction, and operation of the station's critical computer systems, according to an internal NASA technical report. It was first assumed that the failure was a result of external interference, which dictated a remedy in which a power-monitoring device was circumvented on two of the three downed computers with jumper cables. This tactic appeared to work, and analysis teams brainstormed to find the cause of the failure and to determine whether the jumper cable solution was only a temporary fix. The connection pins from the bypassed power-monitoring device were discovered to be wet and corroded, which triggered a "power off" command leading to all three of the allegedly redundant processing units that was designed to shield the units from power glitches beyond the protective capabilities of normal power filters. Water condensation was identified as the source of the corrosion, and the NASA report presumes that the damage was "the result of repeated emissions of condensate from the air separation lines" of a malfunctioning dehumidifier. The Russian engineers' knee-jerk impulse to blame their American partners when the failure occurred is also disheartening. If such a failure occurred on a mission to Mars, the results would probably be lethal to the crew, because they would be out of range of support and resupply missions.

New US Tack to Defend Power Grid
Christian Science Monitor (10/30/07) P. 1; M. Clayton

Despite the US government's efforts to secure the nation's critical infrastructure from cyber attack, hackers as well as attack simulations continue to be more successful, prompting lawmakers to call for a massive overhaul of cybersecurity defenses. "Times are changing very quickly here, and cybersecurity that was good enough even a couple of years ago--the strategy and approach--is obsolete," says US Cyber Consequences Unit director S. Borg. While the greatest concern was once losing control over an infrastructure system such as the power grid, now the biggest threat is that cyber attacks could be used to cause serious physical damage to infrastructure system. Losing control of a system may lead to a loss of power for a few hours or even days, but physical destruction of, for example, an electrical turbine through a cyber attack would be even more devastating. A recently released video by the Idaho National Laboratory demonstrates how a cyber attack could be used to physically destroy a large electrical generator, a technique that could be replicated and adapted to destroy larger and more valuable equipment. "There's a great danger right now that government will spend a lot of money trying to provide better perimeter defenses around the email systems of government, when they should be thinking a lot more about critical infrastructure like the grid," Borg says. To safeguard against such threats US lawmakers are pushing for a new approach. Instead of focusing on building ever-stronger firewalls to keep hackers out, lawmakers want a system that focuses on building infrastructure that can quickly bounce back following an attack. The House Homeland Security subcommittee is expected to unveil a blue-ribbon commission tasked with developing a national cybersecurity strategy to be ready for the next president.

The Air Force's Cyber-Corps
National Journal (10/27/07) Vol. 39, No. 43, P. 56; N. Munro

US officials say that in recent months foreign government-backed hackers have stepped up their attempts to infiltrate or hurt American and other allied information networks. Responses to the many intrusions against some of the 650,000 computers involved in US Air Force operations are handled by the Network Warfare and Ops Squadron, which uses an arsenal of software to counter each attack, no matter how seemingly trivial. Most of the members of this squadron are private contractors, and a new corps of cyber-warriors must be trained to take up the slack. This is the objective of the Air Force Cyberspace Command, which will be organized under the leadership of Maj. Gen. W. Lord. He says the new command must also be prepared to take the cyber-battle to the enemy by infiltrating or crippling enemy networks, should it receive a presidential directive to do so. The command headquarters will likely be comprised of several hundred personnel managing perhaps 20,000 Air Force staffers, which will include lawyers, software specialists, behavioral scientists, and electronic-warfare and satellite experts, Lord says. The unit will provide prowess to the Pentagon's combat commands rather than guide combat operations. The command will also benefit the Air Force by enabling it to better compete with the other armed services for funding and prominent roles in future cyber-warfare commands, says FTI managing director M. Rasch.

Hacker Curriculum: How Hackers Learn Networking
IEEE Distributed Systems Online (10/07), S. Bratus

The hacker community has devised effective methods for the analysis, reverse engineering, testing, and modification of software and hardware, and it behooves leaders in industry and academia to understand this culture and be cognizant of its values, unique strengths, and weaknesses, writes Dartmouth College's S. Bratus. He observes that many quirks of the hacker culture are rooted in frustration with certain industry and academic trends (pressure to follow standard solutions, a limited perspective of the API, a dearth of tools for studying the state of a system, etc.), which he believes contribute to the current abundance of software vulnerabilities. This in turn fuels the hacker culture's impetus to fully comprehend underlying standards and systems, which largely formalize hackers' learning and work ethic. Among the sources hackers tap to acquire skills are classic textbooks highly rated by fellow hackers, electronic magazines, online forums dedicated to specific technical areas, source code from released tools, talks and private communications at hacker conventions, and IRC communities. Hackers have a tendency to adopt a cross-layer approach that tracks data through multiple tiers of interfaces, in accordance with three guiding principles. Bratus lists these principles as inspecting the system state or network on all levels down to the bit level; injecting arbitrary data into the system or network; and identifying and second-guessing deployment peculiarities. The author concludes that in many respects, hacker culture "produces impressive results that enrich other computing cultures, and its influence and exchange of ideas with these other cultures are growing. So, understanding the hacker learning experience and approaches is becoming more important day by day."