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

Δελτίο 99
12 Δεκέμβρη 2007

America Already Is in a Cyber War, Analyst Says
National Journal's Technology Daily (11/27/07), M. Posner

The US government has started to implement its plan for securing government and private networks against cyberattacks, former CIA official A. Palowitch said Tuesday during a talk at Georgetown University's Center for Peace and Security Studies. However, Palowitch said that specific details of the program are likely to remain secret. The Defense and Homeland Security Departments are responsible for the national cyber-security initiative, which is tied to the establishment of a US Air Force cyber command in September and the reallocation of $115 million to Homeland Security's cyber division in November. Palowitch said that he agrees with the assessment of Gen. J. Cartwright, vice chairman of the Joint Chiefs of Staff, that the country is already at war in cyberspace, considering there have been about 13,000 direct attacks on federal agencies and 80,000 attempts on Defense systems. Some of the attacks "reduced the US military operational capabilities," Palowitch said.

Cheap Sensors Could Capture Your Every Move
New Scientist (11/26/07), M. Inman

Swiss Federal Institute of Technology researcher R. Adelsberger along with researchers at the Massachusetts Institute of Technology and Mitsubishi Electronic Research Laboratories have developed a cheaper, more versatile motion capture system that can be used outside of a lab or studio. For example, the system can be used when someone is driving or skiing, to make computer animation or movie effects more life-like, and possibly even to help doctors analyze patients undergoing physical therapy. The sensors, about 2.5 centimeters in size, attach to a person's legs and arms and use accelerometers, gyroscopes, and ultrasonic beeps to detect movement. Tiny microphones on the user's torso detect the beeps, which allows a laptop computer in a backpack to calculate the distance to the sensor. In tests, the system was able to calculate the body's joints and movements almost exactly, but did create some "drift" when the system mistakenly thought the body shifted its orientation as a whole. The system does not work for sudden movements because the sensors are not accurate enough, but Adelsberger says they are quickly improving. "I think the biggest impact of this system is in easier data collection in everyday situations," says New York University motion capture expert C. Bregler. Details of the system were presented at ACM's recent SIGGRAPH conference.

Hacker Threat to US Rising
Sacramento Bee (CA) (11/26/07), D. Montgomery

In response to the hundreds of assaults against government computer systems' firewalls on a daily basis, the US military is weaving computer technology into its standard warfare arsenal. Computer-security operations are underway in all branches of the military, and the Air Force is establishing a full-blown Cybercommand. The military's blueprint is the "2006 National Military Strategy for Cyberspace Operations," which includes offensive and defensive strategies. The document is classified, but could include offensive techniques such as immobilizing an enemy's command-and-control networks. The US military and the US government rely on computers to a great extent, which makes both agencies susceptible to everything from network-crippling viruses to illegal intrusions that aim to steal sensitive data. In the 2007 fiscal year, the Dept. of Homeland Security recorded 37,000 reports of attempted breaches on private and federal systems. Moreover, computer control systems that direct public infrastructure elements confront "increasing risks," according to the Government Accountability Office. Thanks to its advanced firewalls and multilayered systems, the United States has prevented attacks that could cause extensive disruption to federal and private institutions. However, many countries have advanced computer operations, and foreign hackers affiliated with hostile governments are often believed to be behind attacks on US systems, according to experts.

Secretary of State Casts Doubt on Future of Electronic Voting
San Francisco Chronicle (12/02/07) P. C7; J. Wildermuth

California Secretary of State D. Bowen says that electronic voting systems used in California are still too unreliable and untrustworthy to be used in the state's elections. Moreover, Bowen doubts whether the electronic voting systems will ever meet the standards she believes are needed in California. Although Bowen says computer scientists may one day develop reliable systems, she says today's machines are not as transparent or auditable as the paper ballot systems they replaced. A rigorous inspection of the state's voting systems found that most of the voting machines were vulnerable to hackers looking to change results or cause mischief, which resulted in Bowen decertifying almost all touch screen systems used in California. Bowen says she would like to see California use optical scan systems, which use a paper ballot and a tallying machine and are already used to count mail ballots in California. Optical scan systems are "old and boring, but cheap and reliable," Bowen says, because the paper ballots make it easy to have a recount. While Bowen's investigation and decisions only involve California, they have had a nationwide impact because many of the same systems are used in other states. "I want to make sure the votes are secure, auditable, and transparent and that every vote is counted as it was cast," Bowen says.

Government-Sponsored Cyberattacks on the Rise, McAfee Says
Network World (11/29/07), J. Brodkin

Governments and groups across the world are harnessing the Internet to mount cyberattacks on their enemies by attacking key systems such as financial markets, electricity, and government computer networks, according to a new report by McAfee. The report, which was created with input from the FBI, NATO, and other intelligence groups, notes that China has been charged with launching attacks against four countries in 2007. The United States and 119 other nations are also believed to be conducting Web espionage operations, reports McAfee. Such assaults are well-organized, well-funded, and can operate on technical, economic, political, and military fronts. Moreover, the attacks have grown so sophisticated that they can evade the radar of government cyber defenses, according to McAfee. D. Marcus of McAfee anticipates the eventual creation of a privatized model, under which governments will authorize cybercriminals to attack enemies, noting that state-sponsored malware has already emerged. Meanwhile, cyberattacks are also a growing threat to online services such as banking and new targets include VoIP and social-networking applications such as Facebook. Malware is also getting more flexible and robust, as demonstrated by the "Storm Worm," and McAfee researchers have seen "the emergence of a complex and sophisticated market for malware." Finally, the report notes that cybercrime tools such as custom-written Trojans and software flaws are available for sale, and that the underground economy that distributes the tools is so competitive that customer service has become a selling point.

Cryptic Messages Boost Data Security
ICT Results (11/28/07)

The first "real-life" application in quantum cryptography was the use of id Quantique's unbreakable data code in the Swiss national elections in October 2007. "Protection of the federal elections is of historical importance in the sense that, after several years of development and experimentation, this will be the first use of a 1 GHz quantum encrypter, which is transparent for the user, and an ordinary fiber-optic line to send data endowed with relevance and purpose," said id Quantique co-founder N. Gisin. Through quantum cryptography, two communicating parties can generate a shared random bit string only they know, which can be used as a key to encode and decode messages. Furthermore, the parties can be almost immediately tipped off when an unauthorized third party is attempting to gain access to the key and take action to counter the intrusion. Accidental data corruption can also be detected, which is an important consideration in the Swiss elections. The elections are just the first step of a plan to set up a pilot quantum communications network in Geneva called SwissQuantum, whose next phase will be the provision of a platform for testing and validating the quantum technologies that will help safeguard future communications networks. Id Quantique is a partner in the SECOQC project, and id Quantique co-founder G. Ribordy says the initiative "makes it possible for id Quantique's engineers to interact with some of the best groups worldwide in the field of quantum cryptography." SECOQC's partners plan to lay the groundwork for a high-security communication network that melds quantum key distribution with elements of classical computer science and cryptography.

The Next Generation of Security Threats
CNet (12/05/07), I. Fried

Security experts warn that hackers are focusing on areas outside of operating systems, with software applications and Web-connected mobile devices emerging as new areas for exploittation. At the most recent Blue Hat security conference, Microsoft security engineer R. Hensing reported that a decline in operating system vulnerabilities is being accompanied by an increase in application vulnerabilities. Experts predict that malware will adopt even more evasive methods, while IronPort Systems executive Tom Gillis says new malware attack techniques are so complex that they could only have been borne out of refined research and development. IronPort suggests that contemporary malware borrows many traits from social networking sites, such as adaptability and reliance on collaboration, while Trojans and malicious software are likely to become "increasingly targeted and short-lived." The emphasis on resilience and redundancy in the Internet's fundamental design makes securing software a challenge for Microsoft and other companies, according to Microsoft Chairman B. Gates. Trends that have supported the growth of the "shadow" economy include a significant increase in economic opportunity concurrent with a decline in the risk of getting caught, especially since the Internet is not restricted by geography and physical jurisdictions, which makes prosecuting hackers very difficult. "You have evolved financial models that are insanely low-risk with shockingly high return," notes security researcher D. Kaminsky. MessageLabs security analyst P. Wood observes a trend of segmentation in the hacking world, in which attacks are the work of multiple parties instead of just one.

Overseas Electronic Voting Pilot Project Announced

Government Computer News (12/05/07), W. Jackson

Overseas voters registered in Okaloosa County, Fla., will have the option of using an electronic absentee voting system in the upcoming general election, say county election officials. The Okaloosa Distance Balloting Project will deploy several kiosk computers and trained pool workers at locations near US military facilities in the United Kingdom, Germany, and Japan to allow as many as 900 voters to cast absentee ballots through a virtual private network. The pilot program was announce on Dec. 5 and is the initial project of the Operation Bring Remote Access to Voters Overseas (BRAVO) Foundation, which wants to establish reliable electronic alternatives to paper-and-mail absentee voting for Americans oversees by the 2016 presidential election. Okaloosa County is home to several military bases and currently has 20,000 registered voters stationed overseas, but there may be as many as 7 million eligible US voters living overseas and some estimates indicate that as many as two-thirds of overseas voters who request ballots, both military and civilian, have not been able to cast their vote in time to be counted in elections. A system from Barcelona-based Scytl Secure Electronic Voting will be used in the program. On-site poll workers will verify the identity of voters, while voting kiosks will be laptops PCs with no hard drive, so no votes will be stored locally. The kiosks will boot up from a CD with Scytl software and will connect through a VPN to a secure server. The software will be reviewed by the Security and Assurance in Information Technology Laboratory at Florida State University, which has tested voting systems throughout Florida.

Forget Sticky Notes, Microsoft Using Inkblots as Password Reminders
Network World (12/04/07), J. Fontana

Microsoft Research's J. Elson and J. Howell are re-examining a project that uses inkblots as visual aids to help computer users remember complicated and difficult to crack passwords. Using a public Web-based project at InkblotPassword.com, the researchers let users create a password using a series of random inkblots and a formula that selects letters. A series of inkblots are shown to the user, who associates a word with each inkblot. For each inkblot, the user enters the first and last letter of the word the user associates with that inkblot. A series of 10 inkblots creates a password 20 characters long of seemingly random letters that is easily remembered by the user but difficult to steal. After a period of time, users were even able to remember the password without having to refer back to the inkblot, according to research first conducted in 2004. Typically, passwords as complex and secure as the inkblot passwords need to be written down or users will create weaker passwords that are easier to remember. The researchers found that different users almost always describe the same inkblot in different ways, making the system is even more secure and difficult to guess, as users create mental images they associate with the inkblots. Eventually, the users develop "muscle memory" and can log in without referring to the inkblot images.

QUT Researcher Eyes Off a Biometric Future
Queensland University of Technology (12/04/07), S. Hutchinson

Queensland University of Technology researcher S. Phang is developing iris-scanning technology that can be used for such everyday tasks as unlocking homes or accessing bank accounts. "By using iris recognition it is possible to confirm the identity of a person based on who the person is rather than what the person possesses, such as an ID card or password," Phang says. "It is already being used around the world and it is possible that within the next 10-20 years it will be part of our everyday lives." However, today's Iris-scanning technology is limited by such factors as changing lighting conditions. Phang is developing technology that estimates the change in the iris pattern as a result of changes in surrounding light conditions. Using a high-speed camera that can capture up to 1200 images per second, it is possible to track the iris surface's movements to examine how the iris pattern changes depending on the variation of pupil sizes caused by light. Phang says that her study found that everyone has unique iris surface movement, and that it is possible to estimate the change on the surface of the iris and account for how iris features change in different lighting.

EU Focuses R&D on Counterterrorism
Federal Computer Week (12/03/07) Vol. 21, No. 39, P. 42; B. Robinson

The European Union's 7th Framework Program for Research and Development features a homeland security component, giving the EU a larger security technology development agenda than it had previously. The program is an attempt to calibrate EU's security research initiative with separate EU member states' own security R&D efforts. "We do not want the incredible duplication of effort in other research sectors, and we do not want the low level of effecttiveness we see in defense spending brought into this field," said European commissioner for enterprise and industry G. Verheugen at the EU Security Research Conference. "We want value for money." More than $2 billion in annual security R&D would be allocated each year under the program, which represents a 15-fold increase in the amount apportioned in the previous budget. Security research will concentrate on a quartet of objectives, including securing utilities and infrastructures, offering protection from crime and terrorism, border security, and border restoration in the event of a crisis. T.-K. Liem with the European Commission's Directorate-General for Enterprise said the EU security program has two goals--guaranteeing Europe's safety, security, and freedom; and making European industry more competitive via collaboration. "The security research program will be one of a number of mutually reinforceing initiatives aimed at reducing the fragmented internal security market for equipment products and services," Liem said.