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

Δελτίο 3
9 Γενάρη 2006

"Security Flaws on the Rise, Questions Remain"
Security Focus (05/01/06); R. Lemos

Pervasive bugs in Web applications contributed to the first major increase in publicized security vulnerabilities in three years, though different databases offer competing figures on the number of security risks discovered in recent years. A recent examination of four major databases consistently indicated a spike in vulnerabilities stemming from easily discovered flaws in Web applications and a doubling of the number of errors found in software, and security analysts believe that such vulnerabilities will not disappear any time soon. The National Institute of Standards and Technology (NIST) has developed the National Vulnerability Database that uses the Common Vulnerability Scoring System to produce a standardized reading of security flaws. Because each of the four databases surveyed uses different cross-referencing techniques and editorial policies, meaningful comparisons are difficult. CERT, which was one of the databases surveyed, reported 5.198 vulnerabilities in 2005, though that finding has been disputed. Whatever the figure, CERT's conclusion that 2005 saw a spike in vulnerabilities is legitimate and widely agreed upon. Most vulnerabilities are not catastrophic, however. "Web-based vulnerabilities are all over the place and they are really easy to find - they are the low-hanging fruit," said Symantec's David Ahmed. "We have had high-profile vulnerabilities, but that is not what is driving this increase." Computer scientists are more concerned with flaws embedded in the software developed by major companies. It should also be noted that any analysis of software vulnerabilities does not concern products developed in the current year. "These numbers are showing the state of practice from a few years ago, rather than what the current state of practice is today," said CERT's J. Havrilla.

"Better Robots Could Help Save Disaster Victims"
New Scientist (05/01/06); K. Kleiner

The development of search-and-rescue robots continues to be held back by the lack funding from government and industry, according to W. Whittaker, a roboticist at Carnegie Mellon University in Pittsburgh. Roboticists say new search-and-rescue robots would have been beneficial in efforts to save lives, such as at Sago Mine in Talmansville, where 12 miners died. Although the rescue workers made use of a robot, it was a commercial model that was not designed to navigate a mine, and after moving 21 meters into the tunnel it became bogged down. R. Murphy, director of the Centre for Robot Assisted Search and Rescue at the Univ. of South Florida, describes the robot as being slow, ineffective, and designed more for bomb disposal. Whittaker is designing a robot that would use instruments such as laser rangefinders to create detailed three-dimensional maps of tunnels inside of a mine altered after an accident. His colleague H. Choset plans to give a robot the ability to move like a snake through small spaces in a mine or a building that has collapsed. In addition to monitoring conditions and determining whether it is safe for rescue workers to enter, the next-generation of robots may also allow survivors to talk to rescuers and bring them food, oxygen, and medicine.

"Panel Urges Paper Record of Electronic Votes"
Richmond Times-Dispatch (VA) (06/01/06); T. Whitley

A Virginia legislative subcommittee has recommended that the state test a voting system that creates a paper trail to verify the accuracy of electronic machines, though paper trails may be unnecessary if the electronic machines in a pilot program prove reliable. Subcommittee chairman T. Hugo said that he intends to introduce legislation permanently mandating a paper trail for every vote cast, though the measure is likely to be defeated by election officials and registrars. Under the recommendation, the State Board of Elections will establish a monitoring program in several precincts to compare electronic returns with paper records. A permanent paper trail could be required if officials discover significant inaccuracies, though the pilot program will not begin before 2007. Computer scientist Alex Blakemore, co-founder of Virginia Verified Voting, says the pilot program study needs to be objective to be useful, and "the devil is in the details." Hugo believes that paper records could restore voter confidence in a tarnished election process. Virginia plans to use $30 million in federal funding to replace its punch-card and mechanical lever machines with touch screen and optical-scan systems under the Help America Vote Act. The new machines were used in the statewide election of November, which saw the closest contest in modern history in the race for attorney general. A recount shifted 37 votes from Democrat C. Deeds to his victorious Republican opponent, R. McDonnell.

"Quantum Cryptography: When Your Link Has to Be Really, Really Secure"
EDN Magazine (16/12/05) Vol. 50, No. 26, P. 41; B. Schweber

Quantum cryptography (QC) can deliver utterly secure data transmission through the harnessing of the laws of physics, photon quantum states, and Heisenberg's uncertainty principle. BBN Technologies devised a fully operational, multi-node QC system that has been running for over two years, connecting a trio of Boston-area institutions through a 12-mile loop of unused dark optical fiber. The system, which was developed under a 2002 Defense Advanced Research Projects Agency grant, was based on the random polarization of photons, and subsequent selective polarization filtering and polarization-direction detection. A QC system can be employed for either one-time pad or key-exchange cryptography. The generation of a single photon with known quantum states involves the stimulation of a nonlinear crystal by a laser pump, which consequently creates twin photons with identical quantum states, also known as "entangled" photons. Completing a quantum-encrypted link between sender and receiver requires a setup that includes all-optical, electronic, and electro-optical components, including sources, delay lines, phase shifters, couplers, splitters, and optical fibers that incorporate elements that both do and do not maintain polarization. Although very sophisticated, the system can operate by itself with autocalibration, start-up mode, and self-test mode. Continuous data throughput is also supported. BBN Technologies' Chip Elliott says the next step is to make the systems smaller, cheaper, and more hardware-based.

"Networking Tomorrow's Battlefields"
Military & Aerospace Electronics (12/05) Vol. 16, No. 12, P. 26; J. McHale

Situational awareness will evolve as all battlefield elements - soldiers, commanders, vehicles, etc. - are networked together through a combination of technologies, including Internet Protocol (IP), wireless networking, and software-defined radio. Facilitating network-centric warfare is a goal of the U.S. Army's Warfighter Information Network-Tactical (WIN-T) program, which General Dynamics' B. Weiss says is designed to provide warfighters with "access

to critical battlefield information, seamless connectivity to the global information grid, unified network operations, joint interoperability, and security across a host of platforms and points of presence." WIN-T constitutes a secure, high-bandwidth, wireless communications network that will connect soldiers on the battlefield to voice, data, and video, incorporating intelligence, reconnaissance, surveillance, netted weapons, and the Future Combat Systems. One of the WIN-T program's most challenging aspects is the incorporation of on-the-move technologies - radio, satellite, cellular, and IP capabilities - that maintain warfighters' linkage to the network and each other, regardless of whether they are stationary or moving; this will enable commanders to receive the right information constantly. The Joint Common Decision and Execution Capability (CDEC) system developed by Raytheon Network Centric Systems is described by Raytheon's Thomas Flynn as an IP-enabled, "remoted, distributed, and nondedicated" system of elements networked into a single entity. This will help support interdependent elements and semi-automated operations in tomorrow's battlefield. BAE Systems is developing the Adaptive Joint C4ISR Node (AJCN), which can interoperate with American and coalition systems and support real-time network-centric connectivity. BAE's Matt Merryman says AJCN can establish a wide area network from the air with a common data link that combines command, control, communications, and computer, intelligence, and reconnaissance components.

"Are the Bad Guys Winning?"
Campus Technology (06/01/05) Vol. 19, No. 5, P. 20; D. Gale

Cybersecurity authority E. Spafford is not a big believer in the current strategies for cracking down on electronic vulnerabilities, which have grown by more than 10 a day in 2004 and have increased 20-fold since 1995. In recent testimony before the House Science Committee, Spafford, professor and executive director of the Center for Education and Research in Information Assurance and Security at Purdue University, said no one should be shocked if there are more breaches, defacements, and viruses in the immediate future. "The software and hardware being deployed today have been designed by individuals with little or no security training, using unsafe methods, and then poorly tested," said Spafford. "This is being added to the fault-ridden infrastructure already in place and operated by personnel with insufficient awareness of the risks." Spafford, a former member of the President's Information Technology Advisory Committee, believes systems that are simpler, sturdier, and better-made would solve the problem. However, the revenue stream of hardware and software vendors is based on the regular introduction of new and more powerful products that make systems more complex and vulnerable; and research is focused more on short-term patches rather than on making computer architectures more secure. Spafford says that left unchanged, the current system could implode. Alternatively, the market could start demanding and rewarding vendors that focus on making systems simpler and more secure, or people could limit the use of IT to avoid security problems.