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

Δελτίο 75
23 Μάη 2007

Worm Attacked Voter Database in Notorious Florida District
Computerworld (05/16/07), B. Friedman

A variant of the infamous SQL Slammer Worm struck the computer database infrastructure of Florida's Sarasota County on Oct. 23, 2006, and crippled the network by overwriting the system's administrative password. Oct. 23 was the day people voted early on the US House race in the state's 13th Congressional district between V. Buchanan (R) and C. Jennings (D); the Republican candidate was ultimately declared the winner, but the electoral outcome has been contested, and questions about the worm's possible impact on the results--and the disclosure or non-disclosure of the incident to the parties challenging the election--remain. An incident report filed by Sarasota County reported that the worm infected a server on the county's database system, which then "sent traffic to other database servers on the Internet, and the traffic generated by the infected server rendered the firewall unavailable." The report indicated that the server had never been patched for Slammer, and its operation during the election was something of an embarrassment because the machine was slated to be decommissioned, according to Suncoast Technology Center information security analyst H. Logan. The manufacturer of the touch-screen voting systems used in Sarasota issued a bug warning that the county ignored, and submitted a series of stipulations to the county before its release of the source code to a panel of computer scientists organized to probe the incredibly high number of undervotes recorded on the touch-screen machines in the District 13 congressional election in Sarasota. Both documents were withheld from the legal counsel representing the election's challengers by the Sarasota Election Supervisors office. Logan admitted to the possibility that a worm could be used to hack into the voting system, but strongly doubted that the Oct. 23 attack would have been successful had that been the goal. "Our network doesn't share copper or wire with the Supervisor of Elections' network," he explained.

Using 'Offensive Technologies' to Secure Networks
Network World (05/14/07), B. Brown

Stanford University computer science PhD graduate student T. Garfinkel is a program chair for the First Usenix Workshop on Offensive Technologies (WOOT), which takes place in Boston on Aug. 6. Garfinkel says the term "offensive technologies" applies to developers researching and understanding techniques for exploiting software weaknesses, reverse engineering, information gathering, evading detection, and similar activities. By understanding both offensive technologies and traditional defensive strategies such as intrusion detection, access control, and bug detection and prevention, one better understands computer security. Garfinkel says many computer experts read "black hat" magazines and the code used in attack tools. The problem is that the editorial quality of offensive technology journals is often low and with little peer review and the veracity of claims in such media are often questionable. This lack of quality writing on offensive technologies is a major reason for the WOOT conference, where people with different backgrounds and experiences with attack technologies can share their knowledge and expertise. Garfinkel says future malware will target high value targets such as business intelligence and intellectual property that can be sold offshore where litigation and enforcement could be a challenge. Garfinkel also says the "Wild West

atmosphere" of massive amounts of botnets everywhere is bound to give out at some point, and that the most important thing people can do is to influence CIOs and others purchasing programs to put pressure on vendors to build more secure products.

ACM Group Honors Research Team for Rare Finding in Computer Security
AScribe Newswire (05/16/07)

ACM's Special Interest Group on Algorithms and Computing Theory (SIGACT) announced that A. Razborov and S. Rudich, two computer scientists who developed a rare finding that addresses the P vs. NP Problem, will receive the 2007 Godel Prize for outstanding papers in theoretical computer science at the ACM Symposium on Theory of Computing, which takes place June 11-13, 2007, in San Diego. P vs. NP is a fundamental problem in computer and network security techniques and many security optimization techniques. For years, questions on the limits of proof and computation raised by P vs. NP has hindered computer scientists. These questions affect complex mathematical problems common in creating security solutions for ATM cards, computer passwords, and electronic commerce. In a paper titled "Natural Proofs," originally presented at the ACM Symposium on Theory of Computing in 1994, Razborov and Rudich addressed what is widely considered to be the most important question in computing theory, and is one of seven $1 million reward Prize Problems by the Clay Mathematics Institute in Cambridge, Mass. The question asks if the solution to a question is easily checked, is the problem easy to solve? Razborov and Rudich proved that there is no "Natural Proof" that certain computational problems used in cryptography are hard to solve, and though they are widely thought to be unbreakable, there is no natural proof that they are secure. Such cryptographic methods are critical to electronic commerce. Razborov is the leading researcher at the Russian Academy of Science Steklov Mathematical Institute in Moscow, Russia, and Rudich is an associate professor of computer science at Carnegie Mellon University.

Cyber-War--the Way of the Future?
Times Online (UK) (05/17/07), J. Richards

Cybersecurity experts contend that nations need to prepare for the possibility of inter-governmental cyber-war. This declaration came on the heels of a "distributed denial of service" (DDOS) attack on Estonian government Web sites that Estonia alleged came from Russian authorities. This incident demonstrated that a government "definitely" could mount an attack that would cut off a country's essential services by disabling its computer systems, experts say. The attack would be carried out by a "botnet," an enormous army of commandeered "zombie" computers that overwhelm a selected Web site at the command of a master computer. Experts note that this strategy makes it difficult to distinguish the attack's originators from the botnet's unaware victims. Still, there are ways of stymieing the attacks, such as a router that analyzes Web site traffic patterns and can steer suspicious requests into a "cyber black hole." I. Sharaim, chief security officer at MarkMonitor, says, "The US Dept. of Defense is definitely preparing for something like this." Water, gas, and other essential services are vulnerable to such attacks, as they are dependent on IT, says Tier-3 CEO P. Wollacott. "Whether it's a group of university students setting up a botnet or someone more ideologically motivated, all those possibilities are there," he says.

Wary of Everyware
Chronicle of Higher Education (05/18/07) Vol. 53, No. 37, P. A26; A. Foster

New York University instructor and consultant A. Greenfield articulates his concerns that ubiquitous computing--the proliferation of wireless computers everywhere--could have dramatically negative ramifications for privacy and civil liberties in his book, "Everyware: The Dawning Age of Ubiquitous Computing." "The challenge now is to begin thinking about how we can mold that emergence [of ubiquitous computing] to suit our older prerogatives of personal agency, civil liberty, and simple sanity," Greenfield writes in his book. In an interview, the author notes how he was trained to be skeptical of assertions that the comfort, security, and convenience of new technologies will more than make up for the associated losses in personal autonomy, privacy, or agency. Greenfield calls his book "just one of a broader movement toward user-centered design," and he is hopeful that the text's inclusion in the syllabi of some college engineering programs will encourage more critical perception of ubiquitous computing. He teaches an "urban computing" course that examines how ubiquitous computing will probably affect the city and metropolitan life, and from such studies he has concluded that most personal ubiquitous technologies are causing people to withdraw from public engagement, which could carry serious consequences for big North American cities, and anyone interested in civic life in particular. Greenfield observes that many people interested in engineering are lacking in empathy, perhaps by necessity, but that the increasingly social nature of technology calls for more empathetic engineers.

Cyber Assaults on Estonia Typify a New Battle Tactic
Washington Post (05/19/07) P. A1; Finn, Peter

Estonia, one of the most wired countries in Europe, was recently subjected to massive and coordinated attacks against the country's Web sites, including sites belonging to the government, banks, telecommunications companies, Internet service providers, and news organizations, according to Estonian and foreign officials. Computer security specialists called the attacks against the country's public and private electronic infrastructure unprecedented. The NATO alliance and the European Union have sent technology specialists to Estonia to observe and help during the attacks, which so far have disrupted government email and caused financial institutions to shut down online banking. Security experts and officials have warned that during times of war enemies may launch massive online attacks against a target, and the Dept. of Homeland Security has warned that US networks need to be secured against al-Qaeda hackers. The attacks against Estonia provide an opportunity to observe how such assaults may be executed. Estonia's Minister of Defense J. Aaviksoo said the attacks were massive, well targeted, and well organized. Aaviksoo said about 1 million computers worldwide were used in Botnet attacks that began April 27. By May 1, Estonian Internet service providers were forced to disconnect all customers for 20 seconds to reboot their networks. By May 10, bots were probing Estonian banks, looking for weaknesses, and Estonia's largest bank was forced to shut down all services for an hour and a half. Estonian IT consultant L. Viik called the attacks an attempt to take a country back to the Stone Age, and said in the 21st century a country is no longer defined only by its territory and airspace, but by its electronic infrastructure as well.

New Software Can Identify You from Your Online Habits
New Scientist (05/16/07) Marks, Paul

Microsoft is developing software that will be able to determine the identity of a Web user by analyzing an individual's history of browsing the Web. Speaking at the World Wide Web 2007 Conference in Banff, Canada, last week, software engineer J. Hu from Microsoft's research lab in Beijing and colleagues said analytics software can make use of a wide range of

profiles, such as women's preference for searching the Web for health, medical, and religious information, to perform a probabilistic analysis. Raw information could be obtained from different sources, including cookies, a PC's cache of Web pages, or proxy servers for keeping records of Web surfing history. The software is already accurately guessing gender and age. The researchers plan to continue to refine the software with an eye toward accurately guessing occupations, qualifications, locations, and names as well. "Because of the hierarchical structure--language, country, region, city--we may need to design algorithms to better discriminate between user locations," says Hu's colleague H.-J. Zeng. The research has raised concern among some industry observers who believe the software would violate privacy protections in many countries.