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

Δελτίο 87
21 Αυγούστου 2007

Action Plan to Beat Cyber-crime
Information Today (08/07) Vol. 24, No. 7, P. 24; J. Ashling

The International Telecommunication Union (ITU) recently announced the Global Cybersecurity Agenda, a two-year program to improve users' trust in the security of online transactions. ITU secretary general H. Toure said the agenda would focus on finding technical solutions for every environment, developing interoperable legislative frameworks, building capacity in all relevant areas, establishing appropriate organizational structures, and adopting effective international cooperative measures. The agenda says that because cybercrime is a global problem the solution needs to include a coordinated global response from invested parties, including governments, inter-governmental organizations, the private sector, and the civil society. The limited number of existing frameworks are enforceable only within geographical boundaries, national or regional, which allows criminals to exploit loopholes with impunity as they establish operations in countries without appropriate or enforceable laws. Initially, the objectives of the Global Cybersecurity Agenda appear to be overly ambitious, but because the ITU consists of 191 member countries and more than 700 nongovernmental members, the organization has the reach to cover a full spectrum of interests. The first action will be to establish a High-Level Experts Group (HLEG) to refine the goals, identify emerging threats, and develop solutions. The HLEG will produce legislation for interested countries, security and accreditation criteria for software developers, and numerous strategies to assist global cooperation.

USU Lab Researching Cyberterrorism
The Herald Journal (Utah) (08/01/07), K. Burgess

Utah State University researchers in the Space Dynamics Lab's (SDL) Cyberconflict Research Consortium have been researching computer attacks for the past year and a half in an effort to prevent attacks on the United States' technological infrastructure from causing major disruptions. "We would want to avoid the cyber equivalent of Pearl Harbor; that is, something that would catch us unprepared," says SDL program manager J. Marshall. The researchers are working with four other institutions on the project, including the University of Nevada, Reno, the University of Miami, Ohio, Norwich University, and the Potomac Institute for Policy Studies think tank. Each institution is addressing a different aspect of cyber security. The lab's main objective is representing cyber terrorism data in a visual format using visualization and computer graphic images. "With a large-scale cyber attack, you have a lot of information, gigabytes and terabytes of information," says USU computer scientist and research assistant R. Erbacher. SDL has experience in visualization because the information collected from telescopes and sensor systems is best represented visually. The USU cyber terrorism researchers will work on representing cyber terrorism data in a visual manner that is easy for military and homeland security officers to understand. "Any country can try to attack the US over the network," Erbacher says. "We need to be prepared to defend against them."

Online Underworld
San Francisco Chronicle (07/30/07) P. C1; T. Abate

Over the past few years, international criminals have begun employing computer automation to transform unprotected PCs into law-breaking robots, or "bots." Owners of infected PCs remain unaware of the crime. The trend's scope is alarming, as up to 18,000 bands of infected PCs, or "bot nets," are in existence at any given time, according to A. Di Mino of Shadowserver Foundation. Di Mino says security professionals believe there are roughly 8-10 million compromised systems being controlled by "bot-herders." Intent on making money, these criminals are stealthier than hackers of the past. To carry out attacks on Web sites, steal from bank accounts on a large scale, and automate identity theft, the criminals have specialized in various skills. While some criminals create malware, others employ the malware in contaminating PCs, and still others negotiate bot-herding deals. Firewalls can provide PCs with a certain amount of protection, but phishing attacks can fool email recipients into opening tainted files that seem to come from a trusted source. Microsoft has worked to enhance the security in Windows, but bot herders are now instigating their attacks from Web 2.0 platforms. By dodging legitimate Web sites' security features, bot herders infect the sites with malware. Experts wonder whether small Web 2.0 startups will be able to fulfill high security standards, such as those used by Google.

Teaching Hacking Helps Students, Professors Say
Register (UK) (08/07/07), J. Lemos

City College of San Francisco computer science professor S. Bowne said he did not encounter any problems in his ethical hacking class, during a presentation at the DEFCON 2007 hacking conference. Bowne said most of the students who took the course, "Ethical Hacking and Network Defense," were in their 30s and 40s, had children, were not interested in being hackers, and saw the information as helping them in their jobs. He said there was one student who did not follow the course material, but added that this failing student was still helpful in that he maintained all the computers in the lab. Some security firms and universities have sought to limit such courses to computer intrusion and cybercrime for fear that they may one day have to protect their systems and networks from computer science students that they taught hacking strategies. Community colleges have largely embraced the idea, and the courses have improved. Advocates say students gain a better understanding of what risks corporate networks and personal computers face. "It is not so much that you are teaching hacking, but comprehensive security," says L. Johnson, a security analyst with the University of Texas at San Antonio. "If you teach only defensive security, that is not enough."

UC-San Diego Computer Scientists Shed Light on Internet Scams
University of California, San Diego (08/06/07), D. Kane

University of California computer scientists have found significant differences between the infrastructure used to distribute spam and the infrastructure used to host the online scams that profit from spam, a discovery that should help reduce spam and shut down illegal online businesses and malware sites. G. Voelker and S. Savage, both professors at UC San Diego Jacobs School of Engineering, found that while thousands of compromised computers are used to distribute spam, only a handful of individual servers host the scams that spam directs unwary Internet users to. "A given spam campaign may use thousands of mail relay agents to deliver its millions of messages, but only use a single server to handle requests from recipients who respond. A single takedown of a scam server or a spammer redirect can curtail the earning potential of an entire spam campaign," write the UCSD computer scientists in a pa-

per accepted for publication at the USENIX Security conference. Voelker says that the scam infrastructure is critical to the profitability of spam campaigns, and that the current scam infrastructure is particularly vulnerable to common blocking techniques like blacklisting. Using a new approach called "spamscatter," the researchers were able to study over 1 million spam messages from a live feed, and were able to identify URLs in real time and follow the links to the destination server. Then the server location and captured screenshots of the destination Web pages were recorded and grouped together using a technique called "image shingling," which matches visually similar Web pages based on images rendered in a Web browser rather than URL text or spam email content. By identifying Web pages that look alike, the computer scientists identified scams across servers and domains that had shared infrastructure, lifetime, stability, and location, and found that about 94% of scams advertised in spam emails with embedded URLs were hosted on individual Web servers. Of the 6% of scam servers that were distributed across multiple servers, few used more than 10 IP addresses, and one scam used 45 servers. More than half of scam servers identified were located in the United States, 14% were in Western Europe and 13% were in Asia.

A Little Privacy, Please
Scientific American (07/07) Vol. 297, No. 1, P. 92; C. Walter

Director of Carnegie Mellon University's Laboratory for International Data Privacy L. Sweeney is dedicated to upholding people's privacy in an increasingly security-conscious world through the development of software. Her lab has devised "anonymizing" programs that can replace a person's face in a surveillance camera image with a new, impossible-to-identify facial image crafted from other faces in a database. Another brainchild of Sweeney's is the Identity Angel program, which combs the Internet and compiles thousands of identities by connecting names in one database with addresses, ages, and Social Security numbers distributed throughout others--enough information to commit identity theft--so that vulnerable people can be alerted to the problem and take corrective action before they can be exploited by malevolent parties. As a fellow of MIT's National Library of Medicine, Sweeney wrote the Scrub System program to improve the protection of several Boston hospitals' medical records; the program mined patient records, treatment notes, and letters between physicians to extract and delete a greater range of personal patient identifiers than standard search-and-replace software could. According to Sweeney, the ultimate solution is the upfront incurporation of privacy protection into the design and usability of new technologies by engineers and computer scientists. "Society can [then] decide how to turn those controls on and off," she reasons.

Worldwide Malware Study Set for Launch
Dark Reading (08/02/07), T. Wilson

The Worldwide Observatory of Malicious Behavior and Attack Tools (WOMBAT) will gather and correlate malware data from many of the different researchers who study malware and try to identify trends as far as where the malware comes from and how it multiplies. The three-year project, which is scheduled to start in January 2008, has been given a $7.1 million grant by the European Union and corporate sponsors, including France Telecom, Hispasec, and an undisclosed "major security provider." "There are many different groups and projects that track malware, and they can tell us a lot about the malware itself," says S. Zanero, a researcher at the Italian university Politecnico de Milano and founder and CTO of Secure Network. "But they all have flaws, and they don't tell us very much about the people who create the malware. The goal of WOMBAT is to find out the root causes of the observed attacks,

and to use the data we've correlated to help predict upcoming threats." The objective is to see if there is any correlation and to gather data to answer some of questions surrounding Internet security. "Why hasn't the industry seen a major worm attack since 2004? Why has no worm ever targeted the Internet's router infrastructure? Why isn't there more evidence of cyberterrorism? We don't have enough data," says Zanero. WOMBAT has been reviewed and received support from a number of malware research and security groups, including the Internet Motion Sensor, Clearstream, and Hewlett-Packard's Trusted Systems Lab. WOMBAT will begin working at the beginning of 2008, will develop sensors capable of tracking and correlating malware data by 2009, and will complete data analysis by 2010.

California Moves to Lock Down E-Voting Systems
Computerworld (08/04/07), R. McMillan

California is placing some tough restrictions on the use of e-voting systems. Polling stations will be limited to using no more than one of the Diebold AccuVote-TSx and Sequoia Edge Model e-voting systems. Also, county registrars will be responsible for reinstalling the machines' software and firmware, resetting their encryption keys, and implementing measures to guard against physical access to the e-voting systems. The state has similar security measures in place for the use of Hart InterCivic voting machines, except the single-machine restriction. California continues to evaluate Election Systems & Software e-voting machines, which were decertified because the vendor was late in providing access to the systems, and could approve ES&S's products for use in time for the February 2008 elections. Several days before the mandate, the state released a review of the e-voting machines, in which several research teams found a number of security problems in the systems, which enabled them to gain access to the machines and overwrite firmware, bypass locks on systems, forge voter cards, and install a wireless device on the back of a GEMS server.

Prototype Software Tools Plugs Security Leaks
LinuxElectrons (07/31/07)

University of Illinois at Chicago computer security expert V. Venkatakrishnan says that despite assurances from Web browsers that online transactions are secure and will not be intercepted by a third party, often the information is accessible after it enters a merchant's or a bank's computer. Venkatakrishnan, an assistant professor of computer science and co-director of UIC's Center for Research and Instruction in Technologies for Electronic Security, is developing software that will help keep sensitive information private. Venkatakrishnan's software breaks up private, protected data entering programs written in C to separate it from the information that is open to public access. The tool automatically identifies the private and public information, and monitors the program and information flow, like a watchman monitoring two different areas. "Taken together, the public and private zones replace the original functionality of the program," Venkatakrishnan says. "It enables you to enforce different policies on these zones." A prototype of the system has been successfully tested on medium-scale software programs, and Venkatakrishnan received a two-year, $250,000 single-investigator grant from the National Science Foundation to develop a way to scale-up the tool for use on large-scale programs such as mail readers and Web browsers. Venkatakrishnan expects the tool to be tested and ready for public release within two years.

Slicing Sensitive Corporate Data for Secure, Dispersed Storage
Computerworld (08/09/07), T. Weiss

S. Gladwin, who founded the MusicNow online music retrieval and sales service about 10 years ago, believes that he has developed a better way to secure and store sensitive information. Gladwin has developed software that divides critical data into anywhere from four to 128 "slices" that can be stored in either single or multiple data centers. Complex algorithms are used to cut up the data, and a certain number of slices are necessary to make the information readable again. "The data in one location is useless, which makes the transport and storage secure," says Gladwin. The process is similar to packet switching over the Internet, which transmits data in small pieces and reconstructs the information at the other end; but instead of sending the data, it is cut up and stored. Gladwin has made the security process available under an open-source license through a start-up company called Cleversafe. Cleversafe has not yet launched any products and the release of the beta and finished product have not been scheduled; but the company is working to build test networks to prove the technology works. Gladwin says test grids using as many as 300 servers have already been built and used to successfully test the concept. The technology also could be used by banks to ensure secure transactions or by corporate users to grant remote users access through a secure network instead of having them store sensitive information on laptops and portable devices.

Vote-Swapping Over the Internet Is Legal, Court Finds
Computerworld (08/07/07), L. Rosencrance

The Web sites used in the 2000 election to swap votes so voters in swing states who wanted to support the third-party candidate could swap votes with a voter in a safe state who wanted to vote for a major-party candidate have been deemed legal and protected by the First Amendment to the US Constitution by a federal appeals court in California. The purpose of the swap sites, VoteSwap2000.com and VoteExchange2000.com, was to improve Gore's chances of winning the Electoral College without reducing Green Party candidate Ralph Nader's share of the national popular vote, but the site's creators shut down the sites after then-California Secretary of State B. Jones threatened to criminally prosecute VoteSwap2000 .com's owner, A. Porter, for allegedly violating various provisions of the California election and penal codes, including selling votes for money. Porter and VoteExchange2000 .com's owner, W.Cody, shut down the Web sites and filled a lawsuit in federal court claiming that Jones' action of threatening prosecution violated the First Amendment and exceeded his authority under California's election code. The court found that Secretary Jones did exceed his authority and that attempting to stop vote trading, which the court also ruled is not the same as bribing people to vote a certain way, is protected by the First Amendment.