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

Δελτίο 161
30 Οκτώβρη 2009

Prototype Security Software Blocks DDoS Attacks
Network World (10/05/09), T. Greene

Auburn University researchers have developed a software filter that protects computers against distributed denial-of-service (DDoS) attacks without bogging down the computer's CPU and memory. The identity-based privacy-protected access control filter (IPCAF) also wards against session hijacking, dictionary attacks, and man-in-the-middle attacks. Instead of warding against IP addresses, which can be faked by hijackers, IPCAF sends a user ID and password to computer users and the Web site they are attempting to access. Then the two parties create fake ID and values for each packet so that each one is double-checked. Computers check the value in each packet and choose whether to accept it or not. Only then are more memory and CPU resources used to deal with them. The researchers say that IPCAF also is useful because it does not rely on separate and expensive applications that bog down memory. Instead it uses servers and client machines without affecting computer use. IPCAF uses hash-based message authentication code to create the value it will use to confirm every single packet, which saves CPU power, says Auburn's C.-H. Wu. When testing IPCAF, Wu found that the computer network was only stalled by 30 nanosec during an attack through a 10Gbps connection. "For humans, there is no difference," he says. Meanwhile, security teams can possibly track the source of the original attack.

Household Robots Do Not Protect Users' Security and Privacy, Researchers Say
UW News (10/08/09), H. Hickey

A new University of Washington (UW) study has found that domestic robots present security and privacy risks for their owners. The researchers examined three household robots on the market as of October 2008, two of which can be controlled online. The researchers discovered that all three robots could be located using their wireless networks, their audio and video data could be interrupted or even stolen online, they did not always warn people that someone was accessing them, and they did not always alert nearby people to their presence. Moreover, the researchers found that in some cases a robot could be manipulated to hurt its owner or its owner's property. "In the future people may have multiple robots in the home that are much more capable and sophisticated," says UW doctoral student T. Denning. "Security and privacy risks with future household robots will likely be more severe, which is why we need to start addressing robot security and privacy today." The researchers say the solution could be as simple as encrypting wireless networks or removing the robots' Internet access. "People know to look for small parts in children's toys, or look for lead paint," says study co-author C. Matuszek. "For products that combine more advanced technology and wireless capabilities, people should look at whether it protects privacy and security."

Seeking Privacy in the Clouds
Duke University News & Communications (10/13/09), M. Basgall

Duke University professor L. Cox recently received a 3-year $498.000 US National Science Foundation grant to research alternatives for providing social networking services that do not

concentrate all user information in a single place. Cox believes creating a peer-to-peer architecture to spread the information out would make individual data harder to steal or exploit. "The basic idea is that users would control and store their own information and then share it directly with their friends instead of it being mediated through a site like Facebook," he says. In a report for ACM's Workshop for Online Social Networks, Cox proposed three possible options. In each option, users would load personal information into a virtual individual server (VIS), which could be hosted on the user's computer or be distributed within redundant clouds of servers. One of the options is called hybrid decentralization, which would keep VIS on desktops when possible, but switch to the cloud distribution option when individual computers go offline. "Users can try to put their information in clouds of servers, which are going to be highly available but expensive," Cox says. "Or they could try to store it on their own machines, which would be cheap but subject to service interruptions."

Q&A: Defcon's J. Moss on Cybersecurity, Government's Role
CNet (10/16/09), E. Mills

Defcon founder and organizer J. Moss, who was named to the US Homeland Security Advisory Council in June, notes that there is a desire in the US Department of Homeland Security (DHS) and other agencies to augment the cybersecurity alert system as well as adopt Web 2.0 technologies. "It goes back to this theme I keep hearing from people there that they need to fully engage in the cyber area with distributing information," he says. "They want to be more transparent and they want to communicate information faster to broader audiences in different ways. The hang-up seems to be, what are the best ways to do it?" Moss says that DHS has been authorized to hire as many as 1,000 cybersecurity employees over the next three years, but he does not think that specialists are available in such numbers. Moss says agencies' fierce protection of their bureaucratic fiefdoms plays a part in the US government's inability to respond adequately to a cyberattack. He acknowledges that the position of cybersecurity czar has been marked by a lot of turnover, and he presents a theory that "the longer you go without a czar the more they realize that maybe they don't need one, that what they envision what a czar doing, the role is changing." Moss argues that the position should be one tasked with coordinating intelligence, civilians, and the military. "So it's probably more important to get the right person and explain the position so they don't end up with one of these 'all the responsibilities and none of the authority' situations, which is what it sounded like, [a] multiple reporting structure with little budget and little staff and no real authority," he says.

Tracking Devious Phishing Websites
Technology Review (10/16/09), E. Naone

Internet security experts have discovered that many phishers are using a trick called a flux, which allows a fake Web site to rapidly change its URL, making it difficult for defenders to block phishing sites or warn unsuspecting users. New research has found that about 10% of phishing sites are now using flux. Indiana University professor M. Gupta says that because phishers often have access to thousands of hijacked machines they can quickly move a site around the Internet, protecting it from security professionals while keeping the fake site operational. To use a flux, phishers must control a domain name, giving them the right to control its name server. The phisher can then set the name server so it directs each new visitor to a different set of machines, rapidly cycling through the thousands of addresses available within its botnet. If the name server also is moved to different locations on the Internet, it is particularly difficult for defenders to pinpoint a central location where the fake site can be shut down. Gupta has identified several methods for detecting a flux and suggests that flux detec-

tion should be incorporated into the domain name system itself, because only a fraudulent site is likely to use a flux. There are some legitimate reasons for using a flux, but a legitimate flux looks different from a flux on a botnet. Shortening the detection time of phishing sites by even a few hours can make a major difference and make the scams less profitable for criminals, Gupta says.

UAB International Conference Focuses on Preventing High-Capacity Computer Data Theft, University of Alabama at Birmingham (10/14/09), A. Hayenga

At the recent International Conference on Applied Modeling and Information Security Systems, high-performance computing researchers cautioned that worldwide computer use puts a growing amount of digitally stored modeling, design, and supercomputer-processed projects at risk for theft by hackers and called for renewed vigilance in field-related data security. "Modeling and computing helps to solve the world's complex problems, but the information we process on the high-speed devices of our field can easily be abused if lost to those with ill intent," says B. Soni of the University of Alabama at Birmingham, which hosted the conference. "That is why our conference has focused on securing the data we generate as researchers." At the conference, applied modeling information security experts gave lectures on the strategies for securing high-performance computing data, with an overall theme of creating awareness for the threat of data theft. "Now when we work to generate new information and data, we will know to protect it," says Eastern Illinois University professor and conference chair S. Dey. "The information developed in computer modeling is the intellectual property of the researchers and designers, and we do not want it abused."

Field Experiment on a Robust Hierarchical Metropolitan Quantum Cryptography Network, Science in China Press (10/16/09), H. ZhengFu

The University of Science and Technology of China recently demonstrated a metropolitan quantum cryptography network (QCN) for use by the government in Wuhu, China. The researchers say that combining quantum key distribution (QKD) with a "one-time pad" algorithm can create unconditionally secure communication between users. With that objective in mind, the researchers built a QCN that uses a hierarchical structure with multiple levels and three different existing networking techniques. In the Wuhu QCN, nodes with different priorities and demands are set in the central backbone net or the subnet, and assigned suitable networking methods. All QKD links are based on the BB84 protocol with decoy state method, which provides security for the network. The Wuhu WCN runs the Faraday-Michelson interferometer system, which is a unidirectional QKD scheme capable of auto-compensating for the influence of the birefringence in the transmitting channel, which can jeopardize the performance of QKD systems. Several demonstrations of the QCN show that the stability and robustness of the QKD device is sufficient for practical applications. The researchers say that quantum cryptography should eliminate security issues such as hackers and Trojans.

NSF's Cyber-Network Now Expands Across the Northern Hemisphere and Connects Half the Globe, National Science Foundation (10/14/09), L.-J. Zgorski

The Taj network, funded by the US National Science Foundation (NSF), has expanded to the Global Ring Network for Advanced Application Development (GLORIAD), and now connects India, Singapore, Vietnam, and Egypt to the GLODRIAD global infrastructure. The Taj network will support every knowledge discipline, including high-energy physics, atomspheric and climate change science, renewable energy, nuclear nonproliferation, genomics, medi-

cine, economics, and history. The population of countries with access to the NSF-sponsored GLORIAD program now exceeds half the world. "Science is increasingly data driven and collaborative, and does not respect national borders," says NSF's E. Seidel. "High speed optical networks are critical to both national and international scientific efforts." NSF's B. Change says the Taj network provides a new model of international cooperation, will make sharing global network management tasks easy, and focuses on user-leave performance. The Taj expansion significantly extends GLORIAD's existing research and education network and upgrades existing US-China network service from 2.5 Gbps to 10 Gbps, allowing for the placement of high capacity network applications on dedicated lightpaths. Taj principal investigator G. Cole says the network dramatically expands the world's science infrastructure by connecting scientists, educators, and students with the most advanced services available.

Vulnerability Seen in Amazon's Cloud-Computing
Technology Review (10/23/09), D. Talbot

A new study by researchers from the Massachusetts Institute of Technology (MIT) and the University of California, San Diego (UCSD) suggests that leading cloud-computing services may be vulnerable to eavesdropping and malicious attacks. The study found that it may be possible for attackers to accurately map where a target's data is physically located within the cloud and use various strategies to collect data. MIT postdoctoral researcher E. Tromer says the vulnerabilities uncovered in the study, which only tested Amazon.com's Elastic Computer Cloud (EC2) service, are likely present in current virtualization technology and will affect other cloud providers. The attack used in the study involves first determining which physical servers a victim is using within a cloud, implanting a virus on those servers, and then attacking the victim. The researchers demonstrated that once the malicious virtual machine is on the target's server, the malware can carefully monitor how access to resources fluctuates, potentially allowing the attacker to glimpse sensitive information about the victim. The attack capitalizes on the fact that virtual machines still have IP addresses visible to anyone within the cloud. The researchers found that nearby addresses often share the same physical hardware within the cloud, so an attack can set up numerous virtual machines, look at their IP addresses, and determine which ones share a server as the target. It may even be possible to detect the victim's passwords using a keystroke attack, Tromer says. Amazon's K. Kinton says that Amazon has deployed safeguards that prevent attackers from using the techniques described in the study.

To Protect Your Privacy, Hand Over Your Data
New Scientist (10/22/09), V. Venkatraman

A new proposal from the Massachusetts Institute of Technology's (MIT's) Human Dynamics Laboratory suggests that digital identities would be more secure if they were based on data collected from "reality mining," which studies how people behave using the digital data produced by computerized activities. MIT researcher A. Pentland says that researchers and corporations have already realized the potential for reality mining, and argues that if people were to gain control over their own personal data mines they could use that information to prove who they are or inform smart recommendation systems. Pentland believes that allowing access to that data is safer than relying on key-like codes and numbers, which can be stolen or faked. He proposes creating a central body--supported by cell phone networks, banks, and the government--that would manage a data identity system. Banks could provide pieces of data to a third party running a check on a person's identity, and individuals could use their own data for services such as apps on a smartphone. Pentland says such a system would be far

more powerful than existing recommender systems. He has been working to alleviate concerns over using personal data as an identification system, and has gotten the Harvard Law Lab and the World Economic Forum to develop and support the idea. He says 70 other industry partners have expressed interest and will be asked to test a design for the system.