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

Δελτίο 114
30 Απρίλη 2008

Malicious Microprocessor Opens New Doors for Attack
IDG News Service (04/15/08), R. McMillan

Hackers can attack a microprocessor in order to gain unauthorized access to a computer system, according to researchers at the University of Illinois at Urbana-Champaign. The team demonstrated the attack on April 15 during the Usenix Workshop on Large-Scale Exploits and Emergent Threats, a conference for security researchers held in San Francisco. The researchers used a special processor running the Linux operating system, programmed it to launch malicious firmware, then used a special login password to log into the machine. "This is like the ultimate back door," says S. King, an assistant professor in the university's computer science department. "There were no software bugs exploited." Criminals who want to employ this strategy in the real world would have to figure out how to get a malicious CPU onto someone's machine. The US Dept. of Defense warned of such an attack in a February 2005 report, and off-shoring could give hackers an opportunity to attack a PC's microprocessor. Such an attack would be nearly undetectable, but the team also has plans to develop tools that could identify a malicious processor.

Security Experts Split on 'Cyberterrorism' Threat
Reuters (04/16/08), M. Trevelyan

International experts in attendance at the security conference at the Royal United Services Institute in London called for increased cooperation to fight threats to computer networks, such as the botnet attacks that paralyzed Web sites and caused severe disruptions to key services in Estonia last year. "No one country can stand alone in facing cyber attacks and threats," said H. Jazri, the director of CyberSecurity Malaysia. He added that cyberspace is borderless and that attacks typically do not originate from within a country. That was the case with the attack on the Estonian computer networks last year, which the country's government believes was perpetrated by Russia after a diplomatic dispute over Estonia's decision to move a Soviet era war memorial. However, Estonian defense ministry official C.-M. Liflander said it has been difficult to prove who sponsored the attacks. He added that he believed such attacks represent the beginning of an era of cyber terror and possibly cyber war. But S. Cummings of the British government's Center for the Protection of National Infrastructure said he saw no evidence that terrorists were using cyber attacks to wreak havoc on certain countries. He added that he believed talk of cyberterrorism--which he called a "myth"--could distract people from addressing the real risks from electronic attacks.

Positioning Systems Used by iPhone and iPod Breached
ETH Life (04/17/08), R. Cosby

Researchers at ETH Zurich have shown that Skyhook's WiFi Positioning System (WPS) and similar public WLAN positioning systems are vulnerable to location spoofing attacks. Under Skyhook's localization process, Apple iPods or iPhones find their position by detecting neighboring access points, and send this information to Skyhook servers. After the servers return the access point locations to the iPod or iPhone, the device computes its location based on this data. However, the devices have to report detected Media Access Control addresses, which can be forged by rogue access points and easily impersonated. In addition, the access point signals can be jammed and those in the vicinity of the devices can be eliminated. ETH Zurich professor S. Capkun and colleagues were able to impersonate access points from a known location and jam signals sent by access points in the vicinity to eliminate them, which ultimately shows that location spoofing attacks were possible. "Given the relative simplicity of the performed attacks, it is clear that the use of WLAN-based public localization systems, such as Skyhook's WPS, should be restricted in security and safety-critical applications," Capkun says.

Robots, Games, Hackers: First IT-Olympics at Iowa State Celebrates Computer Smarts
Iowa State University News Service (04/16/08), D. Jacobson

About 200 high school students from Iowa will gather at Iowa State University for the first IT-Olympics. The competition, on April 25-26, will include three events. The first is to build LEGO robots that can push, flip, and fight each other in a gladiatorial event. The second event is to create video games that teach a science, technology, or math concept to middle schoolers. The third is to build computer networks that must then be protected from teams of hackers. The event is intended to show students that information technology can lead to interesting studies, good jobs, and creative challenges. The competition is part of a larger Iowa State program called IT-Adventures that is trying to build interest in computer careers by establishing high school IT clubs throughout Iowa. The program provides free computers, mentors, and learning materials. So far, 40 IT clubs have been established. "The students were already interested in computers," says N. Peterman, a teacher at Kuemper Catholic High School. "But this competition expands their exposure to computers. It helps give them an idea if that's a direction they want to go." Organizers say the IT-Olympics will help students see that there is a strong demand for workers with computer and technology skills.

FBI Organizes Defense Against Cyber-Attacks
United Press International (04/21/08), S. Waterman

Last summer, the FBI quietly assembled the National Cyber Investigative Joint Task Force, a group that includes intelligence, law-enforcement, and US government agencies charged with detecting and fighting cyberthreats against the United States. "A network can be attacked by a terrorist group, a foreign power, or a hacker kid from Oklahoma City," says S. Henry, the FBI's deputy assistant director of its cyberdivision. "Networks need to be protected from all threats because once [sensitive] data has been stolen, it can be transferred anywhere." The group operates out of an undisclosed location in the Washington area. The Dept. of Homeland Security released documents in early April that indicated that members of the Secret Service and several other agencies would be added to the task force as well. The FBI also asked for another 70 agents and over 100 support personnel to be assigned to its cyberdivision next year. "We're sharing investigative and threat information," Henry says. "Looking at the attacks [each agency is] seeing and the methodologies being used." He says the group looks at all cyberthreats, but is focused on those that threaten US infrastructure. Moreover, despite recent Congressional testimony by Director of National Intelligence M. McConnell, which identified Russia and China as the US's chief cyber-adversaries, Henry says the task force is "adversary neutral."

Congressman to Press on With Paper-Ballot Emergency Voting Bill

Computerworld (04/18/08), T. Weiss

Rep. R. Holt (D-N.J.) says the House's recent failure to pass the Emergency Assistance for Secure Elections Act will not slow his efforts to get the bill passed. Holt says the bill will make the nation's elections more accurate and secure by helping states transition from direct recording electronic (DRE) machines to systems with paper ballots. "I'm still hopeful that it's possible to get some of this done before this year's November elections," Holt says. "Anything we can do to reduce the unresolved questions and disputes this November we should do." The bill would provide federal funding to states and municipalities to switch from DRE machines to paper-based systems. Holt says the bill is an optional program that would reimburse districts for switching to paper-ballot systems. The White House issued a statement saying the administration "strongly opposes" the bill because it would create a program that is largely redundant with existing law. Holt says there is still some support for such a measure in the Senate, which could allow the House to revisit the issue. "I wouldn't say it's dead for this year, but unfortunately, the window is open only a crack," Holt says.

Researchers Tout 'Functional Encryption' That Knows Who's Who
Network World (04/21/08), E. Messmer

University of California, Los Angeles researchers have developed a new cryptography method called "functional encryption" that makes use of elliptic-curve encryption to secure stored data. "The mathematical system will produce an encrypted record that only people matching the criteria can decrypt," says UCLA professor A. Sahai. "To do this, you get a personalized key that expresses your attributes bound up in one key." A user's key would be able to decrypt the data because the data, which is always stored in encrypted form, uses a mathematical process to recognize anyone with the right key and the appropriate attributes for accessing the data. Sahai says the user is recognized through the math included in the message. He says the goal is to improve server-based security to the point that the server has no idea what it is holding while still enabling authorized people to obtain the data through the mathematics of the security system. Sahai says a new version of the security tool will be available for review so experts can test its efficacy.

To Defeat a Malicious Botnet, Build a Friendly One
New Scientist (04/22/08), M. Inman

University of Washington computer scientists want to create swarms of good computers to neutralize hostile computers, which they say is an inexpensive way to handle botnets of any size. Current botnet countermeasures are being overwhelmed by the growing size of botnets, the researchers say, but creating swarms of good computers could neutralize distributed denial-of-service attacks. The UW system, called Phalanx, uses its own large network of computers to shield the protected server. Instead of accessing the server directly, all information passes through the herd of "mailbox" computers. The good botnet computers only pass information when the server requests it, allowing the server to work at its own pace instead of being flooded by requests. Phalanx also requires computers requesting information from the server to solve a computational puzzle, which takes a small amount of time for a normal Web user but significantly slows down a zombie computer that sends numerous requests. The researchers simulated an attack by a million-computer botnet on a server protected by a network of 7,200 mailbox computers running Phalanx. Even when the majority of mailbox computers were under attack, the server was able to run normally.