UDC 004.056.57 (043.2)

Ruslan SYNYELNIKOV
National Aviation University, Kyiv

COMPUTER SECURITY SYSTEM: THREATS AND VULNERABILITIES

In computer security, the term "vulnerability" is used to describe a flaw in a system that can be exploited to deliberately compromise its integrity and cause it to malfunction. Vulnerability can be the result of programming errors, flaws in system design, insecure passwords, viruses and other malicious programs, script and SQL injections. To comprehend the strategies for a computer security system, it's imperative to initially grasp the different forms of «attacks» that may be launched against it. These threats can generally be categorised into seven main groups: denial of service attacks, social engineering and human error, indirect attacks, eavesdropping, backdoors, exploits, and direct access attacks. Some vulnerabilities are known only theoretically, while others are actively exploited and have known exploits.

An exploit is any unauthorised and illegal attack that exploits a vulnerability in software, networks or hardware. An attack is usually carried out using a computer program, a piece of software code or a sequence of commands to take control of a system, disrupt its operation or obtain data stored on the network. Exploits are caused by errors in the software development process that result in vulnerabilities in the software security system that are successfully exploited by cybercriminals to gain unrestricted access to the software itself and, through it, to the entire computer. Exploits are classified according to the type of vulnerability the hacker exploits: zero-day, DoS, spoofing or XXS. Of course, software developers will soon release security updates to address the flaws found, but until then, the program is still vulnerable to attackers.

Eavesdropping is the secret or surreptitious listening to the private conversations or communications of others without their consent in order to gather information. Even closed systems devoid of external contacts can be eavesdropped on by monitoring weak electromagnetic signals from the hardware. The FBI's proposed Carnivore program is aimed at moving as an eavesdropping system.

Social engineering and human error demonstrate that a computer system is only as private as the people running it. Attackers exploit the carelessness of gullible people or deliberately deceive them, often posing as system administrators and soliciting passwords.

Denial of service attacks, distinct from other exploits,are not aimed at gaining unauthorised access, but at disabling a system. Attackers can overload a machine or network, blocking users, or deny service to individual victims. Distributed denial of service (DDoS) attacks use numerous compromised hosts,forming a botnet controlled by malware, to flood a target system with network requests, attempting resource exhaustion.

Indirect attacks, launched by a third-party computer, complicate tracking the actual attacker. Attackers might exploit public anonymisation systems to conceal their identity.

Backdoors provide unauthorised access to a computer system, bypassing normal authentication and securing remote access. Root-kits, a characteristic shape of backdoors, replace system binaries and smuggle away the presence of other users, services and programs.

Direct access attacks entail utilizing ordinary devices to covertly transfer data. Attackers can install devices like key-loggers or covert listening devices to accommodation security or download large data quantities onto backup media. Encrypting storage media and storing keys separately is a vital defence against such attacks.

Scientific supervisor: Halyna MAKSYMOVYCH,
Senior Lecturer

UDC 656 (043.2)

Sofia SMIRNOVA
National Aviation University, Kyiv

MANAGEMENT OF CLOSED SUPPLY CHAINS: PROBLEMS, PERPECTIVES, INTERNATIONAL EXPERIENCE

The management of closed supply chains includes the coordination and optimization of all processes and resources that interact from suppliers to end consumers. It is an important strategic function for the business and aims to