**Branch :- Computer Sci. & Engg. Class :- Final Year**

**Subject :-System and Software Security Lab manual Sem :- VII**

**Teacher Manual**

**PRACTICAL NO 1**

**AIM**: Understand the essential concepts of system and software security

**THEORY:-**

**What is System Security?**

System security describes the controls and safeguards that an organization takes to ensure its networks and resources are safe from downtime, interference or malicious intrusion. If data security is meant to protect the information in the books in the library, then system security is what protects the library itself.

The security of a computer system is a crucial task. It is a process of ensuring the confidentiality and integrity of the OS. Security is one of most important as well as the major task in order to keep all the threats or other malicious tasks or attacks or program away from the computer’s software system.

A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of various malicious threats and unauthorized access.

The security of a system can be threatened via two violations:

* **Threat:** A program that has the potential to cause serious damage to the system.
* **Attack:** An attempt to break security and make unauthorized use of an asset.

Security violations affecting the system can be categorized as malicious and accidental threats:

* **Malicious threats:** As the name suggests are a kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors and security breaches.
* **Accidental Threats**: On the other hand, are comparatively easier to be protected against. Example: [Denial of Service DDoS attack](https://www.geeksforgeeks.org/computer-network-denial-of-service-ddos-attack/).

Security can be compromised via any of the breaches mentioned:

* **Breach of confidentiality:** This type of violation involves the unauthorized reading of data.
* **Breach of integrity:** This violation involves unauthorized modification of data.
* **Breach of availability:** It involves unauthorized destruction of data.
* **Theft of service:** It involves the unauthorized use of resources.
* **Denial of service:** It involves preventing legitimate use of the system. As mentioned before, such attacks can be accidental in nature.

**Security System Goal:**

**Integrity:**   
The objects in the system mustn’t be accessed by any unauthorized user & any user not having sufficient rights should not be allowed to modify the important system files and resources.

**Secrecy:**   
The objects of the system must be accessible only to a limited number of authorized users. Not everyone should be able to view the system files.

**Availability:**   
All the resources of the system must be accessible to all the authorized users i.e. only one user/process should not have the right to hog all the system resources. If such kind of situation occurs, denial of service could happen. In this kind of situation, malware might hog the resources for itself & thus preventing the legitimate processes from accessing the system resources.

**Types of System Threats:**

**1. Worm:**   
An infection program that spreads through networks. Unlike a virus, they target mainly LANs. A computer affected by a worm attacks the target system and writes a small program “hook” on it. This hook is further used to copy the worm to the target computer. This process repeats recursively, and soon enough all the systems of the LAN are affected. It uses the spawn mechanism to duplicate itself. The worm spawn copies of itself, using up a majority of system resources and also locking out all other processes.

**2. Port Scanning:**   
It is a means by which the cracker identifies the vulnerabilities of the system to attack. It is an automated process that involves creating a TCP/IP connection to a specific port. To protect the identity of the attacker, port scanning attacks are launched from **Zombie Systems**, that is systems that were previously independent systems that are also serving their owners while being used for such notorious purposes.

**3. Denial of Service:**   
Such attacks aren’t aimed for the purpose of collecting information or destroying system files. Rather, they are used for disrupting the legitimate use of a system or facility.

These attacks are generally network-based. They fall into two categories:

1. Attacks in this first category use so many system resources that no useful work can be performed.  For example, downloading a file from a website that proceeds to use all available CPU time.
2. Attacks in the second category involve disrupting the network of the facility. These attacks are a result of the abuse of some fundamental TCP/IP principles.

**What is Software Security?**

In the general sense, security is “the state of being free from danger or threat”. The security of software systems in particular is a vast topic. [Software security](https://www.synopsys.com/blogs/software-security/software-security/) is the application of techniques that assess, mitigate, and protect software systems from vulnerabilities. These techniques ensure that software continues to function and are safe from attacks. Developing secure software involves considering security at every stage of the life cycle. The major goal is to identify flaws and defects as early as possible.

**What do we want to protect using the Software Security?**

* **Data Loss**

This basically means that sensitive data is lost due to security breach. In other words due to a vulnerability in the system someone cracked the system and made an important data disappeared.

A common example is attacker gains access to the main Database and deletes records.

* **Disruption of Service**

This is when the system activity is disrupted due to attackers actions. In this case it may be nothing to do with system data but system go down. The bottom line is the attacker wants the system to stop working. The common example for this is executing a [denial of service](https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/) attack which overloads the system makes it go down. In other means group of attackers can orchestrate huge load of traffic to the system makes its infrastructure overloaded and in turn makes it go down.

* **Data Leak**

This occurs when the sensitive data is stolen and made it available to unauthorized recipients such as credit card information, contact details. Imagine your own credit card details are in the hands of some hackers.

* **Data Inconsistency**

This occurs when data is manipulated by unauthorized attackers and become inconsistent. Attackers can impersonate as someone else and perform unauthorized actions.

**What are the Tool Use for Software Security?**

* **Wireshark**

Wireshark is a [free and open-source](https://en.wikipedia.org/wiki/Free_and_open-source_software) [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](https://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis, software and [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.[[5]](https://en.wikipedia.org/wiki/Wireshark#cite_note-5)

Wireshark is [cross-platform](https://en.wikipedia.org/wiki/Cross-platform), using the [Qt](https://en.wikipedia.org/wiki/Qt_(software)) [widget toolkit](https://en.wikipedia.org/wiki/Widget_toolkit) in current releases to implement its user interface, and using [pcap](https://en.wikipedia.org/wiki/Pcap) to capture packets; it runs on [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS), [BSD](https://en.wikipedia.org/wiki/BSD), [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)), some other [Unix-like](https://en.wikipedia.org/wiki/Unix-like) operating systems, and [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows). There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are [free software](https://en.wikipedia.org/wiki/Free_software), released under the terms of the [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) version 2 or any later version.

* **Nessus**

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks.

The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems.

**CONCLUSION:-** Thus, we have understood the essential concepts of system and software security.