UNIT V
HARDWARE SECURITY

5.1 Hardware security

Hardware security is vulnerability protection that comes in the form of a physical device rather than software that's installed on the hardware of a computer system.

Hardware security can pertain to a device used to scan a system or monitor network traffic. Common examples include hardware firewalls and proxy servers. Less common examples include hardware security modules that provision cryptographic keys for critical functions such as encryption, decryption and authentication for various systems. Hardware systems can provide stronger security than software and can also include an additional layer of security for mission-critical systems.

The term *hardware security* also refers to the protection of physical systems from harm. Equipment destruction attacks, for example, focus on computing devices and networked noncomputing devices, such as those found in machine-to-machine or internet of things (IoT) environments. These environments provide connectivity and communications to large numbers of hardware devices that must be protected through either hardware- or software-based security.

Hardware security is just as important as software security. To assess the security of a hardware device, it's necessary to consider vulnerabilities existing from its manufacture as well as other potential sources, such as running code and the device's data input/output, or I/O, on a network. Although any device should be protected if it connects even indirectly to the internet, the stringency of that protection should match the need. For example, a system controlling the color and intensity of lights in Wi-Fi LED for a dwelling might not require much security.

In the case of more significant hardware and more critical functions, the added reliability and lower number of vulnerabilities associated with hardware-based security might make it advisable. Critical infrastructure includes systems, networks and assets whose continuous function is deemed necessary to ensure the security of a given nation, its economy, and the public's health and safety. Critical infrastructure security is a growing area of concern around the world.

Types of hardware attacks

Gaining access to physical devices isn't as easy as conducting software-based attacks -- such as malware, phishing or hacking attacks -- but over time, cybercriminals have found ways to target hardware. While the use of a default password across multiple devices, outdated firmware and a lack of encryption are the biggest threats to hardware security, other tailored attacks are equally as dangerous.

The following are common types of hardware attacks and what they entail:

- **Side-channel attack.** This attack is notorious for stealing information indirectly, or via side channels. By taking advantage of patterns of information, these attacks analyze the electric emissions from a computer's monitor or hard drive to check for discrepancies in normal emissions. These discrepancies can include the type of information displayed on the monitor or the varying amounts of power that different hardware components use to carry out processes. Typically, the attack will try to exfiltrate sensitive information, such as cryptographic keys, by measuring coincidental hardware emissions. A side-channel attack is also known as a *sidebar* or an *implementation attack*.
- **Rowhammer attack.** This cyber attack exploits a bug inside dynamic RAM (DRAM) modules manufactured in 2010 and later. Repeated accessing or hammering of the memory cells inside the DRAM releases an electrical charge that flips the neighboring bits from zeros to ones and vice versa. This enables untrusted applications to gain full system security privileges and even bypass security sandboxes that are used to mitigate malicious code from entering and infecting the operating system resources.
- **Timing attack.** This side-channel cybersecurity attack targets cryptosystems. Cybercriminals attempt to compromise a cryptosystem by analyzing the time it takes to respond to different inputs and execute cryptographic functions and algorithms.
- **Evil maid attack.** This attack entails physical access to unattended hardware devices, which the criminals can alter in a stealthy way to gain access to the victim's sensitive data. For example, a criminal might insert a USB device installed with device modification software into a powered-down computer or install a keylogger to record every keystroke the victim types.

Trusted Platform Module (TPM)

The Trusted Platform Module (TPM) technology is designed to provide hardware-based,

security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM. Some of the advantages of using TPM technology are:

- Generate, store, and limit the use of cryptographic keys
- Use it for device authentication by using the TPM's unique RSA key, which is burned into the chip
- Help ensure platform integrity by taking and storing security measurements of the boot process

The most common TPM functions are used for system integrity measurements and for key creation and use. During the boot process of a system, the boot code that is loaded (including firmware and the operating system components) can be measured and recorded in the TPM. The integrity measurements can be used as evidence for how a system started and to make sure that a TPM-based key was used only when the correct software was used to boot the system.

TPM-based keys can be configured in a variety of ways. One option is to make a TPM-based key unavailable outside the TPM. This is good to mitigate phishing attacks because it prevents the key from being copied and used without the TPM. TPM-based keys can also be configured to require an authorization value to use them. If too many incorrect authorization guesses occur, the TPM will activate its dictionary attack logic and prevent further authorization value guesses.