**Topic 3B: Configure BIOS-UEFI:**

**Firmware:** Software that is directly integrated into the hardware. Or it is very close to the hardware. BIOS, UEFI.

**BIOS:** only supports **32-bit** operations, does support **keyboard** only.

**UEFI**: Supports **64**-**bit** **CPU**. Supports **GUI** with **mouse** enabled network functionality and better boot security.

**Access to Firmware:** If you cannot go into firmware settings during boot, you can press **Shift + Restart** button on **Windows login screen.**

**Boot Sequence or Boot Order Priority:** Making the system to boot from which device. Options are: Optical Drives, USB, Fixed Disks (HDDs or SSDs) and Network/PXE.

**USB Permissions:** We can set permission for which port will work and which port to stop work from the BIOS. For example, we can set permission to Keyboard and Mouse port open and others get closed for security reasons.

**Fan Considerations:** We can also adjust fan’s speed from the system settings which comes under the heading **Cooling, Power, or Advanced.**

**Boot Password:** It is the password you need to enter even before OS loads. OS passwords and this password is different.

**Two types of Boot Password: Administrator/Setup Password:** This provides access to system settings like **BIOS/UEFI**. **User/System Password:** This locks the entire system.

**Secure Boot:** A most important feature of **UEFI** which is designed to protect the computer from **malware** that could hijack the boot process. It compares the OS which is currently installed with **Cryptographic Keys** with the keys stored in the system and if the keys do not match, it **stops** the boot process.

**Trusted Platform Module (TPM):** It is a small **chip** on the computer’s motherboard that provides secure storage for sensitive information like **digital certificates,** **cryptographic keys**, and **hashed passwords.** Basically, you can use **Windows BitLocker** with **TPM** to lock the hard disk so that anyone who steals it should enter password or recovery key to access it.

**Hardware Security Modules:** It is a secure device like **USB thumb drive**, that stores **cryptographic keys**. An alternate to **TPMs**.