**CHAPTER-2**

**2.1 Introduction to BIOS/UEFI Firmware:**

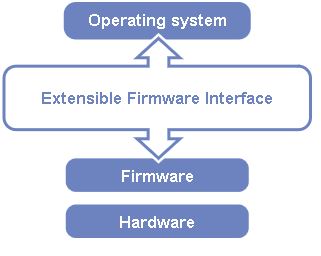
Firmware is a special class of software, so called because it is more or less permanently stored on chips. Nearly every component in a modern PC contains its own firmware. Disk drives, SCSI host adapters, video cards, sound cards, keyboards, and most other devices contain firmware, and nowadays that firmware is seldom read-only. Firmware is held in non-volatile memory devices such as ROM, EPROM, or flash memory. Changing the firmware of a device may rarely or never be done during its lifetime; some firmware memory devices are permanently installed and cannot be changed after manufacture. Common reasons for updating firmware include fixing bugs or adding features to the device. This may require ROM integrated circuits to be physically replaced, or flash memory to be reprogrammed through a special procedure. Firmware such as the ROM BIOS of a personal computer may contain only elementary basic functions of a device and may only provide services to higher-level software. Firmware such as the program of an embedded system may be the only program that will run on the system and provide all of its functions*.*

*[O'RELLY 1.2.3. Firmware Components and the PC BIOS - PC Hardware in a Nutshell, 3rd Edition [Book].htm| https://en.wikipedia.org/wiki/Firmware#Flashing]*

BIOS stands for "Basic" "Input" "Output" "System". When a computer starts (power is first applied) there must be some program code which the CPU executes. This code executes before the operating system (Windows, Linux, etc.) loads. This code is contained in a memory chip(s) on the motherboard. When you start your computer anything you see on the screen before the operating system starts comes from code in the BIOS. This is why if a BIOS update fails or the BIOS become corrupt the computer appears to be dead; there is no code to execute. When BIOS code executes, it establishes a fixed software foundation which allows the operating system to link to the hardware on the motherboard. As CPUs and motherboard technology have become faster and more complex the size and speed of the memory chips required to store the BIOS code have also grown.

[ http://www.arlabs.com/bios\_history.html]

The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. UEFI replaces the Basic Input/output System (BIOS) firmware interface originally present in all IBM PC-compatible personal computers, with most UEFI firmware implementations providing legacy support for BIOS services. UEFI can support remote diagnostics and repair of computers, even with no operating system installed. UEFI boot files are stored in partition which is labeled as EFI. The user can enter a setup utility by pressing their manufacturers specific setup keys.Diagram of Extensible Firmware Interface's position in the software stack is shown below. [ Unified Extensible Firmware Interface - Wikipedia.htm]



*Fig:- Diagram of Extensible Firmware Interface's position in the software stack*

[https://upload.wikimedia.org/wikipedia/commons/4/4e/Efi-simple.svg]

BIOS and UEFI are two firmware interfaces for computers which work as an interpreter between the operating system and the computer firmware. Both of these interfaces are used at the startup of the computer to initialize the hardware components and start the operating system which is stored on the hard drive.

BIOS works by reading the first sector of the hard drive which has the next device’s address to initialize or code to execute. BIOS also select the boot device that needs to be initialized for starting the operating system. Since BIOS has been in use since the very beginning, it still works in 16-bit mode, limiting the amount of code that can be read and executed from the firmware ROM.

UEFI does the same task a little differently. It stores all the information about initialization and startup in an .efi file instead of the firmware. This file is stored on the hard drive inside a special partition called EFI System Partition (ESP). The ESP partition will also contain the boot loader programs for the Operating System installed on the computer.

**2.2 Booting a Computer System:***.*

**2.2.1 Why Booting is Required:**

Hardware doesn’t know where the operating system resides and how to load it. Booting (or booting up) is the initialization of a computerized system. Booting is a process of starting up of an operating system or loading of Operating System into RAM. If booting does not occur you would not be able to use any application on your operating system. Thus booting occurs after you turn on your PC when you see logo of your Operating System.

[https://www.quora.com/Why-is-booting-required-and-when]

*2.2.2 Booting sequence*

**Secure Boot:**