# Module 1

## BOOT THE COMPUTER

- POST
- BIOS and CMOS
- UEFI
- BIOS and UEFI Security
- Update the Firmware

# 1. BOOT THE COMPUTER

## Post

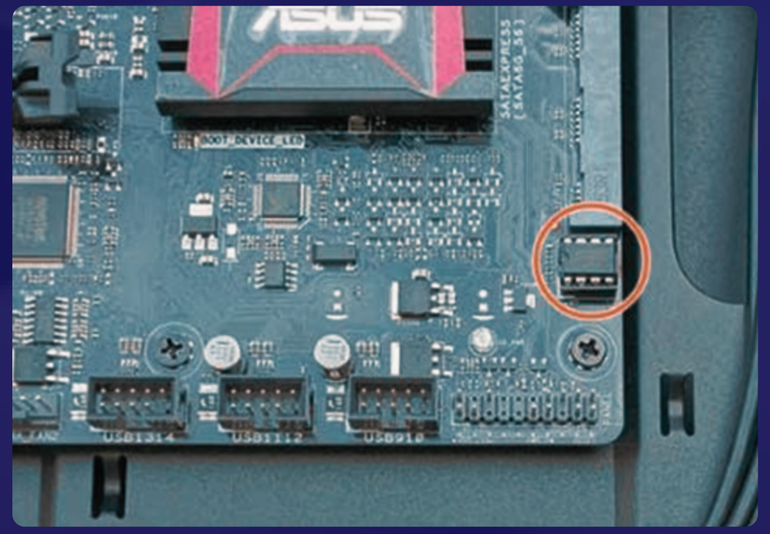
1. The basic input/output system (BIOS) of a computer checks all of its internal parts for hardware issues when it first boots up.
   - The procedure is known as a power-on self-test (POST).
2. A malfunctioning equipment can be identified by an error or beep code, which notifies the technician of the issue.
3. Different BIOS manufacturers use different codes to indicate different hardware problems.
   - Different beep codes may be used by motherboard manufacturers.
   - The motherboard documentation should always be consulted in order to obtain your computer's beep codes.
4. Press the specified key at POST to access the BIOS.
5. Installation Tip: Turn on the computer after removing all of the RAM modules to see if POST is functioning correctly. When a computer lacks RAM installed, it should sound the beep code.

# 1. BOOT THE COMPUTER

## BIOS and CMOS

1. To operate properly, every motherboard requires a BIOS

2. The BIOS, a ROM chip found on motherboards, is a short program that manages how the hardware and operating system communicate with each other.




3. In addition to the POST, BIOS indicates:
   - Which drives are in stock
   - Which drives are bootable
   - How the memory is configured and when it can be used
   - How PCIe and PCI expansion slots are configured
   - How SATA and USB ports are configured
   - Motherboard power management features

4. A Complementary Metal Oxide Semiconductor (CMOS) memory chip stores the motherboard BIOS settings.

# 1. BOOT THE COMPUTER

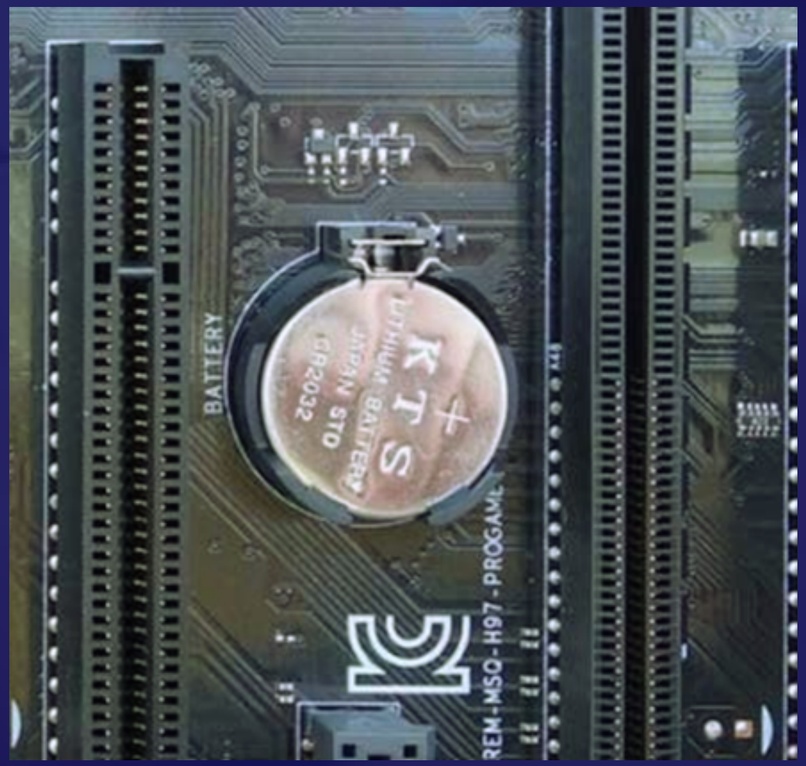
## BIOS and CMOS

5. **The BIOS software determines how to configure the hardware when a computer boots by reading the preset parameters that are saved in the CMOS.**

6. **The BIOS settings are retained by CMOS using a battery.**

7. **If the battery fails, settings can be lost.**

8.**Installation Tip: If the computer’s time and date are incorrect, it could indicate that the CMOS battery is bad or is getting very low.**



# 1. BOOT THE COMPUTER

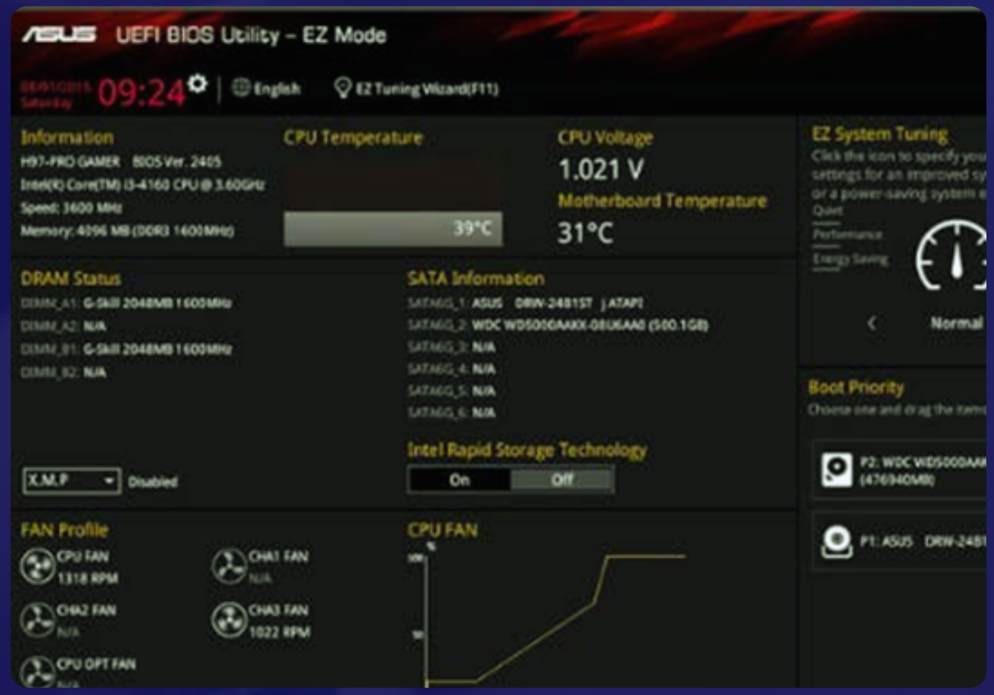
## UEFI

1. **Today, Unified Extensible Firmware Interface (UEFI) is used by themajority of computers**

2. **Every new computer has UEFI, which provides additional features and addresses security issues with legacy BIOS.**

3. **UEFI can run on 32-bit and 64-bit systems, supports larger boot drives, and includes additional features such as secure boot.**

- **Secure boot ensures your computer boots to your specified operating system.**
- **This helps prevent rootkits from taking over the system.**



# 1. BOOT THE COMPUTER

## BIOS and UEFI Security

| Access Level | Level Description |
|---|---|
| Full Access | All screens and settings are available, except the supervisor password setting. |
| Limited Access | Changes can be made to certain settings only, for example, the time and date. |
| View Only Access | All screens are available, but no settings can be changed. |
| No Access | No access is provided to the BIOS setup utility. |

1. The legacy BIOS supports some security features to protect the BIOS setting, however UEFI adds additional security features.

2. The BIOS and UEFI systems have several standard security features, such as:
   - **Passwords-** Different levels of access to the BIOS settings are possible with passwords.
   - **Drive encryption-** For protection against data theft, a hard drive can be encrypted. It prevents data from being read from a hard drive even if the hard drive is moved to another computer.
   - **LoJack-** The owner can use this security feature to find, lock, or remove every file from the device.
   - **Trusted Platform Module (TPM)-** This is a chip designed to secure hardware by storing encryption keys, digital certificates, passwords, and data.
   - **Secure boot-** A UEFI security standard called Secure Boot makes sure that a computer will only boot an operating system that the motherboard manufacturer has certified.

# 1. BOOT THE COMPUTER

## Update the Firmware

1. For the purpose of to improve system performance, compatibility, and stability, motherboard manufacturers may release upgraded BIOS versions.
2. ROM chips held the BIOS data for early computers, and upgrading the BIOS required physically replacing the ROM chip.
3. By using Electronically Erasable Programmable Read Only Memor (EEPROM), users can update modern BIOS chips without having to open the computer casing.
   - This is called flashing the BIOS
4. Visit the manufacturer's website to download a new BIOS, then follow to the suggested installation steps.