Branden, Brice, Tolulope, Kerin
9/12/24
Foundation of Computer Network Security

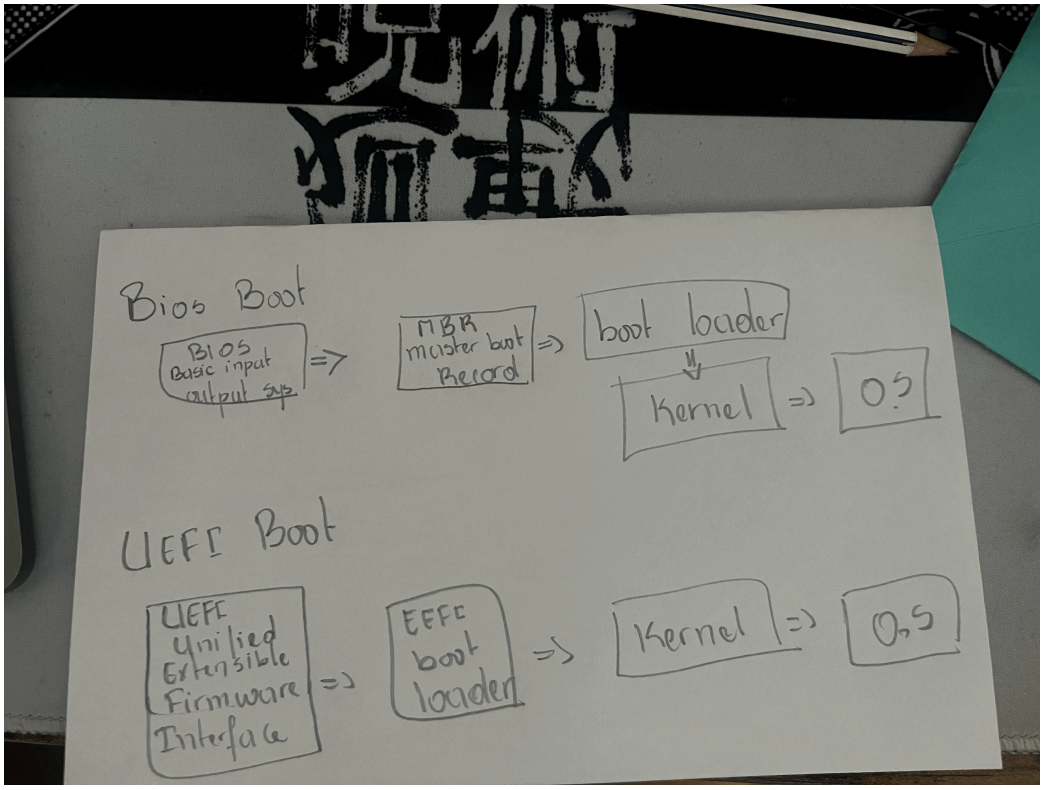
Group Class Assignment

Compare BIOS and UEFI features.

Feature/Term	BIOS (Basic Input/Output System)	UEFI (Unified Extensible Firmware Interface)
POST (Power-On Self-Test)	BIOS performs a hardware check during startup called POST. If it detects any issues, the boot process stops until the issue is resolved.	UEFI also runs a POST but can handle more complex diagnostics and recovery tools if errors occur. It is faster and more advanced than BIOS.
MBR (Master Boot Record)	BIOS uses MBR to organize disk data and locate the operating system. MBR can only support drives up to 2.2 TB and allows a maximum of 4 primary partitions.	UEFI uses GPT (GUID Partition Table), which supports larger storage capacities (over 2.2 TB) and allows more partitions, typically up to 128.
Partitions	BIOS relies on the MBR partition system, which restricts you to four primary partitions. You have to use extended partitions to get more.	UEFI uses GPT, allowing for a larger number of partitions without the need for extended partitions. It can manage larger and more complex storage setups.
Primary Partition	BIOS can only boot from one of the four primary partitions set in the MBR. This limits flexibility in disk management.	UEFI can boot from any partition set in GPT, and because GPT supports many more partitions, it's easier to manage different OS installations.
System Partition	In BIOS, the system partition is part of the MBR, which points to the bootloader that helps start the OS.	UEFI uses a dedicated EFI System Partition (ESP), which holds bootloaders and other important files needed

		to boot the system. It's more organized and reliable.
Active Partition	BIOS requires an active partition to be flagged in MBR to tell the system where to boot from. Only one partition can be active.	UEFI does not rely on the concept of active partitions. Instead, it looks at the EFI System Partition to find boot information, making the process smoother.
Partition Table	BIOS uses MBR for partitioning, which limits disk space and the number of partitions. It's not ideal for modern large drives.	UEFI uses GPT, which is a more advanced partition table format. GPT can handle disks of almost unlimited size and supports many more partitions, making it better for large storage systems.
Boot Loader	BIOS relies on the bootloader stored in the first 512 bytes of the MBR. This space is very limited and makes adding features difficult.	UEFI uses the EFI System Partition to store boot loaders, which gives more space and flexibility. You can easily have multiple boot loaders for different operating systems (e.g., Windows, Linux).
Firmware	BIOS is an older, less efficient firmware. It initializes hardware using 16-bit mode, which slows down the boot process.	UEFI is newer, running in 32-bit or 64-bit mode. It boots faster, handles modern hardware better, and supports more advanced features.
Embedded System	BIOS is sometimes used in older embedded systems, but its limitations make it less common in modern setups.	UEFI is more common in modern embedded systems due to its flexibility, speed, and ability to handle larger systems more effectively.
CMOS	BIOS settings, like system time and hardware configurations, are stored in the CMOS chip, which is battery-powered.	UEFI doesn't need CMOS for storing settings. Instead, it uses non-volatile memory, so settings remain intact even without power.
Secure Boot	BIOS does not support Secure Boot. There is no built-in protection against	UEFI supports Secure Boot, which ensures that only trusted software (like verified

	unauthorized software during startup.	OS components) can boot. This helps prevent malware from starting at boot.
Virtual Machines	BIOS can be emulated in virtual machines, but it has limitations and isn't ideal for modern virtual environments.	UEFI is preferred in virtual machines, offering better support for large disk images, modern hardware features, and Secure Boot even in virtualized environments.



How is secure booting related?
UEFI brought with it a feature called Secure Boot. It makes sure that the only operating systems that can boot are those that have reliable and properly validated certificates. This stops malicious software from being installed at startup and from interfering with the boot process.

How UEFI and BIOS Affect Secure Boot:
BIOS: Secure Boot is not supported by a traditional BIOS. Because it cannot verify the program that is run while booting, boot-time malware attacks can more easily target it.

UEFI: Secure Boot, a feature particular to UEFI, took the place of the previous BIOS. A more secure system environment is produced with UEFI through the use of digital signatures and certificates to authenticate the software that is loaded during the boot process.