13.5.3 BIOS/UEFI Security Facts

Depending on your motherboard, you can configure the following security-related features in the BIOS/UEFI configuration utility:

Feature	Description
Passwords	You can configure passwords in the BIOS/UEFI configuration to control access to the system. - If set, the administrator password (sometimes called the supervisor or setup password) requires the user to authenticate in order to enter the setup program to make changes to BIOS/UEFI configuration. - If set, the user password (sometimes called the system or power on password) requires the user to authenticate in order to boot the operating system. Usually, the administrator password can also be used to start the system. BIOS/UEFI passwords offer only a limited degree of protection. - Passwords can typically be cleared by removing the motherboard battery or setting a motherboard jumper. - If you have set an administrator password and then find the password is no longer set, you know that someone has tampered with the system. - Use a chassis lock to prevent users from opening the case to reset passwords.
Drive Locking	Some motherboards allow you to set a password on the system hard disk. This practice is sometimes referred to as *drive locking*. - When set, the password must be given at system startup or the disk cannot be used. - There are two different passwords: user and master. - Set the password(s) by using the motherboard's BIOS/UEFI configuration program. - Passwords are saved on the hard disk itself. - You cannot read the passwords from the disk. - You cannot move the drive to another system to access the disk without the password (the password moves with the disk). - You cannot format the disk to remove the passwords. - If you forget the user password, use the master password to access the drive. If you do not know either password, you cannot access any data on the drive. - Most drive locking systems allow a limited number of incorrect password attempts. After that time, you must restart the system to try entering additional passwords. - Some systems ship with a default master password already set. However, these passwords (if they exist) are not publicly available and cannot be obtained from disk manufacturers.
Chassis Intrusion Detection	Chassis intrusion detection helps you identify when a system case has been opened. With chassis intrusion detection a sensor switch is located inside the system case. When the case cover is removed, the switch sends a signal to the BIOS/UEFI. Depending on the system configuration, a message might be displayed on the screen at startup, or the message might be visible only from within the BIOS/UEFI configuration program.
Trusted Platform Module (TPM)	A *TPM* is a special chip on the motherboard that generates and stores cryptographic keys. - You can use the BIOS/UEFI configuration program to initialize the TPM. - During initialization, you can set a TPM owner password. The TPM password is required to manage TPM settings. - The TPM includes a unique key on the chip that can be used for hardware system identification. - The TPM can generate a cryptographic key or hash based on the hardware in the system. It then uses this key value to verify that the hardware has not changed. This value can be used to prevent the system from booting if the hardware has changed. - The TPM can be used by applications to generate and save keys that are used with encryption.
LoJack	LoJack is a mechanism that is used to secure systems that are prone to being stolen, such as notebooks systems. The LoJack software is implemented within a chip on the motherboard itself and you can use it to recover a stolen system. The LoJack service running on the computer periodically contacts a LoJack server at the vendor's site to:

	▪ Report its current location using GPS coordinates. ▪ Query LoJack headquarters to see if that system's been reported as stolen. If the system has been reported as stolen, then LoJack will continuously update the server with its current location, making it easier for law enforcement to figure out where it is. The software that performs these two tasks is not actually contained in the motherboard chip. The software contained in the motherboard chip is just a downloader that downloads and installs the LoJack software as a Windows service.
UEFI-Specific Security Features	UEFI systems include several security features that are not available on BIOS-based systems: ▪ UEFI requires firmware updates to be digitally signed by the hardware vendor. Using digital signatures, unauthorized changes to firmware updates (such as the insertion of malware) can be detected. ▪ UEFI provides a security feature called SecureBoot, which requires the operating system installed on the system hard drive to be digitally signed. If it isn't digitally signed, then the UEFI firmware will not boot it by default. This is designed to block a special type of malware called a rootkit. A rootkit inserts itself into the boot sector of a storage device, causing it to be loaded first. Then the rootkit loads the actual operating system. By doing this, the rootkit gets loaded before any anti-malware software, making it more difficult to detect. SecureBoot also prevents the booting of unauthorized operating systems. For example, it prevents the system from booting an operating system installed on a removable USB drive that could be used to access data on the system hard drive.