**Module 3 Architecture & Design**

**3.3 Systems Design**

**Hardware/Firmware Security**

* FDE (Full Disk Encryption) – Bitlocker, Veracrypt
* SED (Self-Encrypting Drive)

1. Automatically encrypts/decrypts drive
2. Media Encryption Key (MEK)
3. Key Encryption Key (KEK) – supplied by user

* TPM (Trusted Platform Modules)

1. Specialised chip on endpoint device that stores encryption keys specific to host system for hardware authentication
2. Usually on system motherboard

* HSM (Hardware Security Modules)

1. Physical computing device that safeguards & manages digital keys for strong authentication & provides crypto processing
2. Traditionally come in form of plug-in card/external device that attaches directly to computer/network server

* BIOS (Basic Input/Output System) – boot-up configuration
* UEFI (Unified Extensible Firmware Interface) – modern boot-up configuration, replacing BIOS
* Secure Boot & Attestation

1. Cryptographic hash of BIOS/UEFI OS boot loader & drivers & compares against stored hash
2. Done to prevent rootkits & boot sector viruses

* Root of Trust (RoT)

1. Highly reliable hardware, firmware & software components that perform specific, critical functions
2. Security process that begins with some unchangeable hardware identity often stored in TPM

* Supply Chain – confirming origin of hardware is secure

**Operating Systems Types**

* Network
* Server – windows server, Linux
* Workstation
* Appliance (AKA IoT) – limited to specific purpose
* Kiosk – public computer
* Mobile OS

**Operating System Security**

* Trusted OS/baseline
* Secure configurations
* Least functionality/single purpose
* Disabling unnecessary ports & services – there are 65535 TCP & UDP ports which are divided into 3 ranges

1. Well-known ports – 0 to 1023
2. Registered ports – 1024 to 49151
3. Dynamic Private ports – 49152 to 65535

* Disabling default accounts/passwords – Windows guest accounts, routers/switches
* App whitelisting/blacklisting
* Patch management process

**Patch Management**

* Patch

1. Set of changes to computer program/its supporting data designed to update/fix/improve it
2. Includes fixing security vulnerabilities & bugs

* Hotfixes – small, specific-purpose updates
* Service Pack – collection of Hotfixes that have been combined
* Updates – provides more comprehensive improvements for features/additional security/adds software enhancements & compatibility
* Upgrades – new version of software

**Peripherals**

* Wireless keyboards
* Wireless mice
* Displays
* Wi-Fi-enabled MicroSD cards
* Printers/MFD (Multi-Function Displays)
* External storage devices
* Mobile devices/smartphones
* Digital cameras