

CIT 270: SYSTEMS SECURITY I

CHAPTER 9: CLIENT AND APPLICATION SECURITY

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

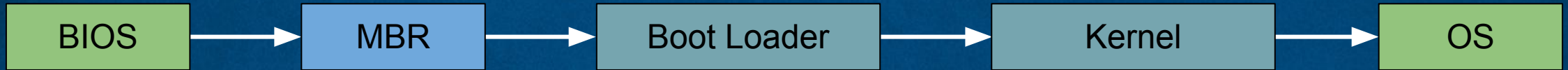
Note 

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to **yellow words**. These highlighted words denote a topic that will almost always be on your chapter quiz.

CLIENT SECURITY: HARDWARE

The **BIOS** (**B**asic **I**ntput / **O**utput **S**ystem) is a chip integrated into the motherboard on early personal computers that would awaken and test the various computer components and then load the operating system.



UEFI (**U**nified **E**xtensible **F**irmware **I**nterface) is integrated into the motherboard and is the first program that runs when a computer is turned on. UEFI has added functionality and security over BIOS. Using **Secure Boot** it insures that only software that is trusted can be booted by checking its digital signature.



CLIENT SECURITY: HARDWARE

UEFI and Secure Boot are part of the **chain of trust** where each element relies on the confirmation of the previous element to know that the entire process is secure.

For this process to truly be secure you need a secure starting point that you can trust. The strongest point in a computer is the integrated hardware that cannot be modified. This is known as the **hardware root of trust** where UEFI and Secure Boot checks are *rooted* in with the initial hardware checks of the computer.

The network that moves a product from the supplier to the customer can be vast and can be susceptible to **supply chain infections** where a product is infected during the manufacturing or storage of that product.

CLIENT SECURITY: SECURING THE OS SOFTWARE

<u>OS Type</u>	<u>Uses</u>	<u>Examples</u>
Network OS	Software that runs on a network device like a firewall, router, or switch.	Cisco Internetwork Operating System (IOS), Juniper JUNOS, MikroTik RouterOS
Server OS	OS software that runs on a network server to provide resources to a network users.	Microsoft Windows Server, Apple macOS Server, Red Hat Linux
Workstation OS	Software that manages hardware and software on a client computer.	Microsoft Windows, Apple macOS, Ubuntu Linux
Appliance OS	OS in firmware designed to manage specific devices; digital recorder or a game console.	Linpus Linux
Kiosk OS	System and user interface software for interactive kiosks.	Microsoft Windows, Google Chrome OS, Apple iOS, Instant WebKiosk, KioWare.
Mobile OS	OS for mobile phones, smartphones, tablets, and other handheld devices	Google Android, Apple iOS, Microsoft Windows mobile

CLIENT SECURITY: SECURING THE OS SOFTWARE

Security of an OS depends on the proper configuration of its built-in security features. A typical OS security configuration should include:

- disabling unnecessary ports and services
- disabling default accounts & passwords
- least functionality; minimum set of permissions
- application whitelisting / blacklisting

Patch: a security patch is a publicly released software security update intended to repair a vulnerability; service pack.

Patch Management Tools can help with patch distribution and patch reception but these come with ethical concerns; Google Chrome.

CLIENT SECURITY: SECURING THE OS SOFTWARE

Antivirus (AV): software that examines a computers files and activity for any infections or viruses; static (signature) and dynamic (heuristic) analysis.

Other software and applications you can use to protect your devices and network include anti-spam and anti-spyware.

Trusted OS: OS hardening is using tightened security during the design and coding of an OS. The resulting OS is now a trusted (hardened) OS.

CLIENT SECURITY: PERIPHERAL DEVICE SECURITY

Secure Digital (SD): a popular type of removable storage that comes in three different form factors: full SD, miniSD, and **microSD**.

The four families of SD are:

1. Standard-Capacity (SDSC)
2. High-Capacity (SDHC)
3. eXtended-Capacity (SDXC)
4. Secure Digital Input Output (SDIO)

Wi-Fi Enabled microSD Card: a popular SDIO device for digital cameras that supports the wireless transmission of data (pictures) across the network.

CLIENT SECURITY: PERIPHERAL DEVICE SECURITY

Multifunctional Device (MFD): combines the functions of a printer, copier, scanner, and fax machine; has a CPU, hard drive, LAN connection, etc.

Although not a comprehensive list you need to be mindful of all kinds of devices you might not normal consider in your security plans:

- Digital Cameras
- External Storage
- Displays

CLIENT SECURITY: PHYSICAL SECURITY

Different types of passive barriers can be used to restrict unwanted individuals or vehicles from entering a secure area:

- Fencing; anti-climb paint, anti-climb collar, roller barrier, rotating spikes
- Signs
- Lighting
- Cages
- Barricades; directing
- Bollard; vehicular traffic
- Security guards
- Video cameras (CCTV)
- Motion detection

CLIENT SECURITY: INTERNAL PHYSICAL SECURITY

In the event that an intruder makes it past external defences you should equally robust internal defences as well:


- screen filter; waiting areas
- door locks; deadbolts
- key management; regulation procedures and tracking
- access logs
- mantraps
- protected distribution systems (PDS); cable conduits
- cable locks
- secure cabinets
- safes / vaults

CLIENT SECURITY: PHYSICAL SECURITY



 Data Center - Security and Risk Management



 Inside a Google Data Center



 Security and Data Protection in a Google Data Center

CLIENT SECURITY: APPLICATION SECURITY

Attacks based on application vulnerabilities:

<u>Attack</u>	<u>Description</u>	<u>Defense</u>
Executable Files Attack	Trick the vulnerable app into modifying or creating executable files on the system.	Prevent the app from creating or modifying executable files for its proper function.
System Tampering	Use the vulnerable app to modify special sensitive areas of the OS (Windows Registry) and take advantage of those modifications.	Do not allow apps to modify special areas of the OS.
Process Spawning Control	Trick the vulnerable app into spawning executable files on the system.	Take away the process spawning ability from the app.

CLIENT SECURITY: APPLICATION SECURITY

New memory vulnerabilities. See chapter 5 for additional vulnerabilities:

<u>Attack</u>	<u>Description</u>	<u>How this is Exploited</u>
Buffer Overflow	An app dynamically allocates memory but does not free that memory when finished with it.	Attacker can take advantage of unexpected program behavior resulting from a low memory condition.
Pointer Dereference	A pointer with a value of NULL is used as if it pointed to a valid memory area.	Launching the program by an attacker can cause the process to crash, resulting in loss of data.
DLL Injection	Inserting code into a running process through a Dynamic Link Library (DLL).	Attacker can use DLL injection vulnerability to cause a program to function in a different way than intended.

CLIENT SECURITY: APPLICATION SECURITY

Developing an application requires several stages:

- **development stage**; requirements
- **testing stage**; security check
- **staging stage**; QoS
- **production stage**

These stages are usually referred to as the **application development lifecycle model** that describes the different stages in creating an application:

- sequential design with the **waterfall model**
- incremental design with the **agile model**

CLIENT SECURITY: APPLICATION SECURITY

One specific type of software methodology is the **Secure DevOps** model that follows the agile model of software development:

- **security automation**; tools that test for vulnerabilities
- **continuous integration**; checking security integration at each stage
- **immutable systems**; locked in configurations or branch to a new system
- **infrastructure as code**; managing resources with same principles as an OS
- **baselining**; clear comparison points to measure goals and success

CLIENT SECURITY: APPLICATION SECURITY

Provisioning is the enterprise-wide configuration, deployment, and management of multiple IT system resources; new app is a resource.

Deprovisioning is the removing of a resource that is no longer needed.

Change Management and/ or **Version Control** is vital when using agile methods.

CLIENT SECURITY: SECURE CODING TECHNIQUES AND TESTING

Read pages 404 – 405.

Table 9-8 is another great handout to have.

REFERENCES

Attacks based on application vulnerabilities [Table 9-6]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 401. Boston, MA: Cengage.

Book [PNG]. Flat Icon. https://www.flaticon.com/free-icon/book-opened-outline-from-top-view_30169

Booting using a BIOS [Figure 9-1]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 376. Boston, MA: Cengage.

“Data Center - Security and Risk Management” Anixter, YouTube, 9 February 2015, <https://youtu.be/8g0NrHExD3g>

“Inside a Google data center” G Suite, YouTube, 16 December 2014, <https://youtu.be/XZmGGAbHqa0>

Link Icon [PNG]. Share Icon. No license found, public domain inferred.

Memory Vulnerabilities [Table 9-7]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 402. Boston, MA: Cengage.

REFERENCES

Paperclip Icon [PNG]. Copenhagen: Icon Finder. SIL Open Font License.

“Security and Data Protection in a Google Data Center” G Suite, YouTube, 18 September 2013,
<https://youtu.be/cLory3qLoY8>

Types of OSs [Table 9-1]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 379. Boston, MA: Cengage.