CSF3404 Cyber Security

Chapter 4
Managing Data, Application, and Host Security

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli
Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

Manage Device and Host Security

- Ensure that devices and hosts using data and applications are secure.
  - To properly protect the assets of the organization as a whole:
    - Must be secured the networks, devices, and end-user systems in the organization.
    - Must be established necessary security measures on all the devices within an organization.

✓ Because most viruses today start from an individual machine first, then spread to other devices through a network.

Hardening

- It is an attempt to close vulnerabilities and generally protect the system against attacks.
- It is implemented to comply with the security requirements in a defined security policy.
- It can also limit the access and capabilities of the system.
  - ✓ So, the balance between accessibility requirements and usability in a particular case is important..

A hardened server

Operating System Security

- Each type of operating system has unique vulnerabilities.
- Systems from different vendors have different weaknesses.
- There can never be a single comprehensive list of vulnerabilities for each operating system.

  - ✓ **Security professionals** should keep abreast of system security and information posted on vendor sites and in other security references.

Operating System Security Settings

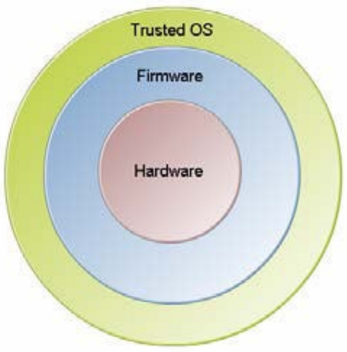
- Managing services running on the operating system.
- Configuring the operating system's built-in firewall.
- Configuring Internet security options.
- Managing all automatic updates and patches for software and services.
- Enabling necessary auditing and logging functions when applicable

Trusted Computing Base

- It is a hardware, firmware, and software component of a computer system that is responsible for ensuring that the security policy is implemented and the system is secure.

- The security properties of an entire system could be jeopardized should a defect occur inside the **TCB**.

- The **TCB** is implemented;
  - In the hardware through processor rings or privileges.
  - In the firmware through driver and resource protection.
  - In the operating system's isolation of resources and services from applications **Trusted Operating System**.



Security Baselines

- It is a collection of security and configuration settings that are to be applied to a particular host in the enterprise.

- The host software baseline is a benchmark against which you can compare other hosts in your network.

- Creating a baseline for a specific computer depends on its operating system and functionality in the organization and should include the manufacturer's recommendations.

- So, it will have separate baselines defined for desktop clients, file and print servers, Domain Name System (DNS)/BIND servers, application servers, directory services servers, and other types of systems.

  ✓ Scan tools for security vulnerabilities: Nessus, Nmap, Microsoft Baseline Security Analyzer (MBSA), and Security Configuration Wizard (SCW).

Software Updates

- **Patch**: A small unit of supplemental code meant to address either a security problem or a functionality flaw in a software package or operating system.

- **Hotfix**: A patch that is often issued on an emergency basis to address a specific security flaw.

- **Rollup**: A collection of previously issued patches and hotfixes, usually meant to be applied to one component of a system, such as a web browser or a particular service.

- **Service Pack**: A larger compilation of system updates that can include functionality enhancements, new features, and typically all patches, updates, and hotfixes issued up to the point of the Service Pack's release.

Application Blacklisting and Whitelisting

- **Application blacklisting** is the practice of preventing the execution of programs that an organization has deemed to be undesirable.

- Prevent blacklisted apps from installing or running on the target system.

- Blacklisting is used in many antiviruses, antispam, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs).

- **Application whitelisting** maintains the list of approved applications.

- Allow the whitelist application to be installed or run on the target system.

- Whitelisting is a good example of the principle of implicit denial.

Logging

- logging is using an operating system or application to record data about activity on a computer.
- Log files themselves can be the target of an attack.
- The resulting log files are usually stored as text files in known locations.
- The level of detail available in log files can vary from showing.
- Reviewing the activity recorded in log files can be difficult due to the variations in formatting and detail.
- The review may reveal a great deal about a suspected attack.

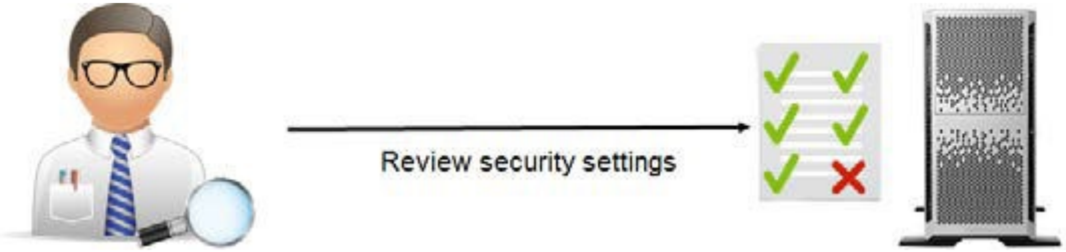
- Log files themselves can be the target of an attack.

Auditing

- It is the process of performing an organized technical assessment of the security strengths and weaknesses of a system.

- Computer security audits can include:
  - ✓ Testing the strength of passwords.
  - ✓ Scanning the network for open ports or rogue servers and workstations.
  - ✓ Reviewing log files ➔ either manually or via software.
  - ✓ Reviewing user and group permissions.
  - ✓ Reviewing the physical security related to the system or systems in question.

A security professional performing an audit



Anti-malware Software

- It is protective software that scans individual computers and entire enterprise networks for known viruses, Trojans, worms, and other malicious programs.

- Some programs attempt to scan for unknown harmful software.

- Types of Anti-malware Software:
  - ✓ Antivirus software.
  - ✓ Anti-spam.
  - ✓ Anti-spyware.
  - ✓ Pop-up blockers.
  - ✓ Host-based firewalls.

Windows Firewall Configuration

- It is a software-based firewall that is included with all current Windows operating system client and server versions.

- Types of Firewall Rules:
  - ✓ **Inbound rules**: Define the action to be performed by the firewall on the data that enters the system from another system.
  - ✓ **Outbound rules**: Define the action to be performed by the firewall on the data that flows out of the system.
  - ✓ **Connection security rules**: Define the type of authentication that is needed to allow communication between the systems.

http://technet.microsoft.com/en-us/library/dd448535(WS.10).aspx

Virtualization Security Techniques

- **Patch management:**

A patch management system must be in place to ensure that all relevant patches are installed.

- **Least privilege:**

The concept of least privilege should be applied when determining access control assignments to any virtual environment.

- **Logging:**

User activities in the virtual environment should be logged and reviewed to check for irregular activity and any possible security breaches.

- **Design:**

Applying good security measures to all virtualization environments starts with a good design.

- **Snapshots:**

Consistently capturing snapshots, or the state a virtual environment is in at a certain point in time.

- **Host availability:**

the availability of a virtual host is dependent on its ability to adapt to various system changes.

- **Sandboxing:**

Is a security mechanism for separating running programs, usually in an effort to mitigate system failures and/or software vulnerabilities from spreading.

Hardware Security Controls

Hardware security controls can be applied to help prevent security issues:

- Proper logoff and shutdown procedures must be enforced for all systems when not in use.
- Wireless communication devices must be approved by the IT department and installed properly.
- Mobile devices, such as laptops, mobile phones, and smartphones, must be properly stored and secured in a cabinet or safe when not in use.
- Cable locks should be installed and used on all end-user hardware components.
- Strong password policies should be enforced on all end-user devices.

Non-standard Hosts

It is operating systems and other computing environments that are not updated or changed, either by design or due to other circumstances such as age.

- Supervisory control and data acquisition (SCADA) systems

A type of industrial control system that monitors and controls industrial processes such as manufacturing and fabrication; infrastructure processes such as power transmission and distribution; and facility processes such as energy consumption and HVAC systems.

- Embedded-software systems

Some hosts, such as game consoles, printers, Smart TVs, and motor vehicles include software that is not meant to be updated or is not normally updated by an IT department.

- Mainframe computers

Highly stable and reliable computers that are used for mission-critical applications and bulk data processing.

- Some mobile devices

Mobile devices such as smartphones and tablets may be considered non-standard hosts if their Android or iOS versions are old enough to no longer be supported by the manufacturer.

Security Controls for Non-standard Hosts

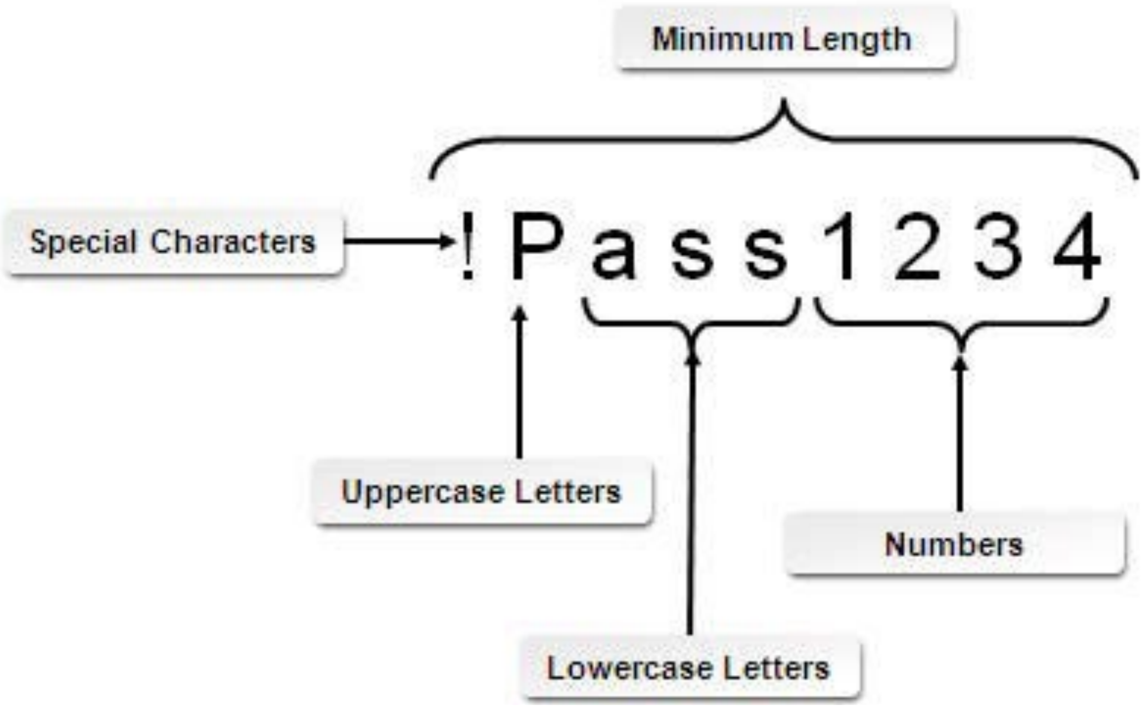
There are a corresponding number of security controls that you might want or need to apply to those hosts, including:

- **Layered security**, including network segmentation and application firewalls, to isolate at-risk systems from the remainder of the network environment.
- **Manual updates** on an ad hoc basis for older versions of Android and iOS.
- **Firmware** version control for SCADA and embedded systems.
- **Wrappers**, which are software that contains other data or software, such as legacy code. Wrappers enable the contained data or software to operate in newer environments.
- **Controlling redundancy** (the provision of multiple identical instances of a system for fault tolerance) and **diversity** (the provision of multiple different implementations of the same specification to minimize common vulnerabilities)

Strong Passwords

A strong password is a password that meets the complexity requirements that are set by a system administrator and documented in a security policy or password policy.

The elements of a strong password



- The minimum length of the password.
- Required characters, such as a combination of letters, numbers, and symbols.
- Forbidden character strings, such as the user account name or dictionary words.

Guidelines for Establishing Device and Host Security

It must implement security measures that protect the devices themselves from attack, and that prevent unauthorized access to your network, while ensuring that legitimate users continue to have the appropriate level of connectivity between internal and external networks.

Device Security Guidelines

- Software-based systems, harden the base operating system to close security holes in running services.
- Hardware-based systems, install the latest firmware updates to address known security issues.
- Implement your hardware and software manufacturers' security recommendations.
- Implement strict access control and use strong, robust passwords.
- Secure router configuration files.
- Configure appropriate ingress and egress filters.
- Disable IP source routing.
- Implement a routing protocol that supports authentication.
- Protect routers with properly configured firewalls.
- To protect against Address Resolution Protocol (ARP) poisoning.
- Implement NAT.
- Close unused well-known ports.
- Place appropriate servers in a demilitarized zone (DMZ).
- Disable IP directed broadcasts on routers.
- Protect all internetwork devices and network media from unauthorized physical access to prevent wiretapping, vandalism, and theft.
- Test the functionality of systems after hardening to make sure that required services and resources are accessible to legitimate users.
- Document your changes.

Host Security Guidelines

- Require strong passwords.
- Implement your hardware and software manufacturers' security recommendations.
- Implement antivirus, anti-spyware, and anti-adware software.
- Disable unnecessary services.
- Restrict access permissions.
- Implement security policies to control, limit, or restrict user interaction with the system.
- Physically secure mission-critical servers and devices by installing them in locked rooms to which only trusted administrators have access.
- Plan backup strategies. Backup media should be stored offsite.
- Test the functionality of systems after hardening.
- Utilize scanning and auditing tools to detect potential vulnerabilities in your systems.
- Identify non-standard hosts and what measures can and need to be taken to protect them against vulnerabilities.
- Document your changes

Manage Mobile Security

- Mobile devices are used everywhere and are deployed by many companies for employees' business use.

- Mobile devices are everywhere today.

- It is important to understand the most common devices used today and what threats and vulnerabilities apply.

- To understand;
  - ✓ What techniques are used to secure mobile devices?
  - ✓ How do they prevent unauthorized access to mobile devices and sensitive data?

Mobile Device Types

- A mobile device is a small handheld computing device. There are a number of common mobile devices used for work purposes today:

- **Smartphones:**

  - ✓ Examples include Apple® iPhones®, BlackBerry® devices, Windows Phone® devices, and Android™ phones.

- **Wi-Fi enabled devices:**

  - ✓ Examples include Apple® iPads®, the Apple® iPod touch®, and Android based tablets such as the Barnes & Noble NOOK Color™.

Mobile Device Vulnerabilities

- Modern mobile phones have the ability to transfer voice data, emails, photos, and videos, and can access the Internet.

- Users can assume all the same threats related to desktop computers and laptops will apply.

- For example, viruses and spam can infect mobile devices.

- Attackers can hack into the mobile device as they would a desktop or laptop computer.

Mobile Device Security Controls

- **There are a number of controls used to provide mobile device security:**
- **Use device management:**
  - ✓ Enables IT admins to securely monitor and manage the mobile devices that access sensitive business data.
- **Enable screen lock:**
  - ✓ Once the device is locked, it can only be accessed by entering the code that the user has set up.
- **Require a strong password:**
  - ✓ A strong password should be set up by the user.
- **Configure device encryption:**
  - ✓ All mobile devices should be configured.
- **Require remote wipe/sanitization/lockout:**
- **Enable global positioning system (GPS) tracking:**
  - ✓ This feature is used as a security measure to protect mobile devices that may be lost or stolen.
- **Enforce access control:**
  - ✓ Implementing authentication and authorization when employees use mobile devices will uphold the principle of least privilege.

Mobile Device Security Controls

- **Enforce application control:**
  - ✓ Setting restrictions on what apps a user can access.
- **Use asset tracking and inventory control:**
  - ✓ There are many ways you can track devices in real-time, such as through GPS or QR codes.
- **Limit removable storage capabilities:**
- **Implement storage segmentation:**
  - ✓ Consider dividing data storage along certain lines (e.g., cloud vs. local) based on your security needs.
- **Disable unused features:**
  - ✓ Every feature has the potential to be another point of vulnerability in a mobile system.

Mobile Application Security Controls

- Encryption and key management
- Credential management
- Authentication and transitive trust
- Restrict geo-tagging:
- Is the process of actively adding geographical identification metadata to an app or its data.
- Application whitelisting:
- Keeping a whitelist of acceptable apps will ensure that your app is not
- compromised by insecure software that is out of your control

Guidelines for Managing Mobile Security

- Familiarize yourself with the different types of mobile devices and operating systems.
- Implement a centralized mechanism for managing devices on your network.
- Enforce screen lock, password input, and other device access features.
- Disable unnecessary features.
- Have a plan for remotely wiping our locking out data in case of theft.
- Enable device-wide encryption, if available.
- Apply some form of access and application control on all devices.
- Manage how data is stored and how data storage should be restricted.
- Keep track of devices and take inventory.
- Consider your employees' BYOD needs.
- Draft rules and regulations that employees must agree to for mobile use, along with general corporate policies.
- Acclimate new employees to these protocols and have a plan for off-boarding former employees.
- Consider the legal issues of BYOD: data ownership, privacy concerns, and how much of their device usage you can control.
- Adjust your system architecture and infrastructure as needed.
- When developing apps, enforce proper encryption and key management protocols.
- Select the proper authentication methods and credential management systems to keep users secure.
- Restrict what your app communicates with and how

Thank you