CS 493
Secure Software Systems

Ch 4 The OS Environment

Dr. Williams
Central Connecticut State University

Objectives

- Operating system security
- The importance of computer operating system security
- Common operating systems
- Hardening the operating system
- Operating system backup and recovery

Goals

- Define computer operating system security.
- Describe common security flaws applicable to operating systems.
- Mitigate the security vulnerabilities in common operating systems.
- Apply disaster and recovery techniques to operating systems.

Why patch timeliness

- Apache Struts2 vulnerability (CVE-2017-5638) disclosed and patched by Apache March 2017
  - Classified severity 10.0 (max)
  - Basic vulnerability on file upload if the content type specified didn't match what app wanted framework throws an exception…
  - Malicious user could craft message so content type rather than being a simple type was XML and in framework error handling was possible to get it to run code inside the XML
- Equifax breach Fall 2017
  - Attacked September using this known attack, patch still not applied
  - 143 million people compromised

What Is Operating System Security?

- An **operating system** is a manager for hardware and software resources on a computer; it controls resource usage and access and provides a means for the user to interact with the computing system (via input devices and a GUI displayed on a monitor).
- The operating system out of the box is not secure without further configuration. You must develop a secure baseline for all of the systems in your organization.

What Is Operating System Security?

- The operating system is where your applications live and access the network if required. Requirements, such as passwords, are often ignored time and time again.
- The operating system connects to the network and from there has the ability to access the Web using the Internet.

Why update/harden continued

- So air gapped don't need to update?
  - Stuxnet purportedly developed by US and Israel between 2005-2012 (neither officially admitted responsibility)
  - Worm taking advantage of 4 zero-days specific target programmable logic controllers (PLCs) of Iran's nuclear centrifuges
  - Machines were air gapped, multiple levels of network isolation for security
  - Worm spread via network and USB, idea slowly spread across network and across isolation boundaries via USB use
  - Hid and avoided detection only spreading until on a machine with access to specific PLC – ruined/destroyed approx. 1/5th of centrifuges

Operating System Threats

Many of the operating system threats arrive via the information system network infrastructure:

- Viruses are malicious code developed to reside and run silently on a user's operating system; they are developed to pass from computer to computer via email or some other way.

Operating System Threats

- **Boot sector virus-** an attack which occurs when the first sector is loaded into memory when the computer is started.
- **Macro virus-** a virus written as a macro to execute malicious code.
- **Polymorphic virus-** a virus type that constantly morphs or changes its footprint to fool virus-detecting software.
- **Worm-** Similar to a virus that has the ability to self replicate while working its way through the network.

Operating System Threats

- **Rootkits** are purposely designed to hide in your operating system by hiding fragments of the executable and deleting detectable fragments after it executes on the intended target, installing itself in parts of the system's registry or master boot record (MBR).

Operating System Defense Tactics

- One of the first steps to hardening your operating system is to develop a multilayered approach to your security strategy.
- You close the gaps and strengthen your walls by finding services you don't use, shutting them down, and making them unviable to an attacker.

Common Operating systems

- Windows
- Mac OS
- Unix
- Solaris
- Linux

While all of these OSs have been successfully attacked many times, Unix/Linux variants generally accepted as more secure due to finer levels of control available to harden the systems

Windows

- Windows 7 and later come with **BitLocker®** available with the enterprise and Ultimate editions and enable the user to encrypt the entire hard drive.
- UAC notifies the user of any changes or attempts to change the system by an application.
- Internet Explorer®8 and later now come with a feature called SmartScreen® that checks all of the sites you visit against a database to ensure that you are visiting a safe, legitimate site. This filter also protects your system against (**some**) cross-site scripting.

Mac OS X Snow Leopard

There are many industry publications that can help an organization harden its operating systems. NIST, for example, puts out updated OS-hardening checklists that can help you with this task, and the following URLs identify organizations that produce a wealth of information:

- Defense Information Systems Agency (DISA): http://iase.disa.mil/stigs/index.html
- National Institute of Standards and Technology (NIST): http://csrc.nist.gov/itsec/ guidance_W2Kpro.html
- National Security Agency (NSA): http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml

Mac OS X Snow Leopard

- Never use the administrator account to conduct daily tasks, such as surfing the Web or checking your email.
- Anyone with malicious intent can easily defeat all other password mechanisms unless you have the firmware password set.
- In system preferences settings on a Mac you can also disable automatic log-in by setting the automatic log-in to the Off position. It is also important to disable the sharing for guest accounts by unchecking the selection.

Mac OS X Snow Leopard

- Mac OS X also includes two firewalls that include a packet-filtering and an application version.
- The packet-filtering firewall requires some expertise, though instructions can readily be found on the Apple website in the *Mac OS X Security Configuration* guide.
- The built-in camera and microphone should be disabled, if needed, because these hardware devices can be compromised.

Linux

We can't forget the usual practices that you should start with when implementing a Linux-based system:

- Create user accounts using strong passwords.
- Just as when using a Mac, do not work off of the administrator or root account to conduct non-administrator tasks.
- Review your system logs and store them on a server.
- Encrypt log-in information.
- Encrypt critical data transmissions to avoid interception.

Linux

- You should set up your BIOS to disable booting from external devices and set a password for the boot loader. Because Linux works on open source code, you should be very careful when downloading applications of an unknown origin.
- Turn off any unnecessary services.

Linux

- Linux also has several encryption options available for encrypting any portion of the media or file system. For file encryption, you can use GPG (GnuPG), which is a single file-encryption tool.

Auditing and Monitoring

- Monitoring and auditing changes that occur in an information system are crucial to effectively managing security in an organization's infrastructure.
- Auditing requires that a written policy be established that determines and dictates how and which events will be archived.
- Auditing and monitoring help you to identify a baseline for resource usage.

Backup and Redundancy

- Data backups and redundancy procedures are a critical piece of the operating system environment.
- Server redundancy can be achieved by maintaining a redundant server that can be mirrored and housed many miles away.
- An organization can have an entire site—complete with servers, data, and power—many hundreds of miles away or a continent away that stands by, ready to take over operations in the event of such a disaster.

Backup and Redundancy

There are three types of data backups that should be noted:

- **Full backup:** Make an entire copy of all of the data from the target drive.
- **Differential backup:** Make copies of all files that have changed since the last full backup.
- **Incremental backup:** Copy only changed files since the last full backup.

Full backup strategy

- Full backup of all files from the target drive
- Pro
  - Easy to recover quickly from any specific day
- Con
  - Typically very slow with large systems sometimes taking longer than 24 hours
  - Large amount of data storage needed
    - If take full backup 7 days a week need storage for 7x the size of the active system for just a week's worth of back ups!

Differential backup strategy

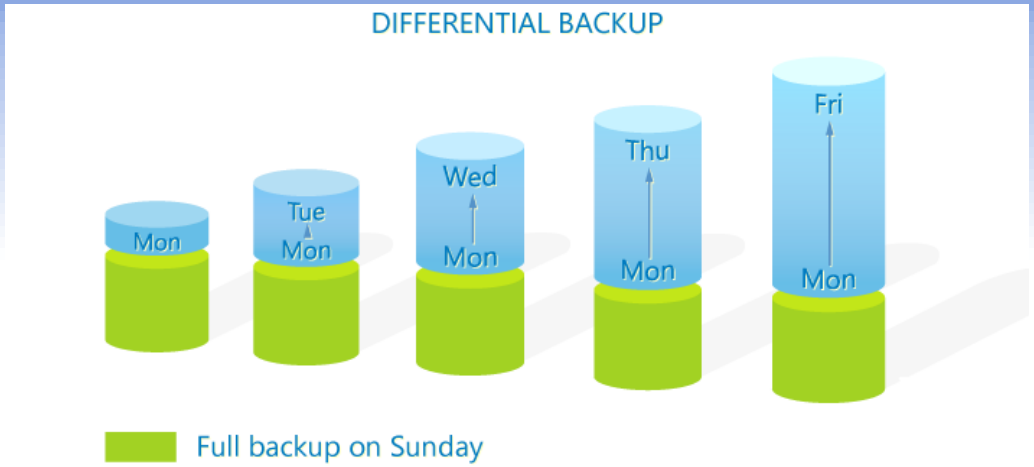

Image from codetwo.com

- Full back up taken periodically
- Each subsequent back up until next full back up stores all files that changed **since the last full** back up
- Pros
  - Much faster than full backup
  - Backup giving daily recovery per week much smaller than full backup approach
- Cons
  - If time between full backups is long difference for day can get large potentially as large as full back up
- Recovery applied by taking last full then applying difference file for day to restore to

Increment backup strategy

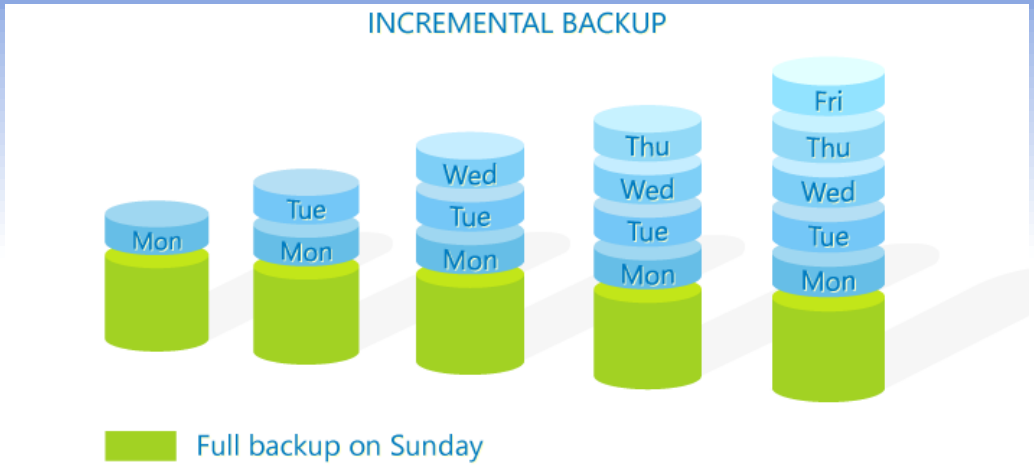

Image from codetwo.com

- Full back up taken periodically
- Each subsequent back up until next full back up stores files that changed **since the last incremental** back up
- Pros
  - Much faster than full backup, typically much faster than differential – Can allow smaller timeframes such as down to hourly backups
  - Backup giving daily recovery per week much smaller than full backup approach, typically much smaller than differential as well as only small amount each time
- Cons
  - Recovery applied by taking last full then applying differences to files in sum of back ups forward to restore point – so can be more lengthy recovery
  - In some cases if single increment is lost impossible to restore (incremental) back up after that point

Backup and Redundancy

Many operating systems have the ability to use a process for fault tolerance protection known as **Redundant Array of Independent Drives (RAID).**

- **RAID Level 0:** Does not provide fault tolerance, but simply improves read and write performance by using **disk striping,** which spreads blocks of data across the disk array.
- **RAID Level 1:** Uses disk mirroring to provide fault tolerance.
- **Disk mirroring** is the use of several drives connected to the same RAID disk controller, which sends the duplicate data to the other disks in the RAID to create a mirror of the data. This gives the administrator the ability to remove a faulty disk and continue operations without loss of data. Level 1 is slower on write operations.
- **RAID Level 5:** Uses multiple drives, but stores error-checking data, known as parity data, on all drives in the array instead of just one, providing an additional layer of protection. This level is one of the most popular for new system implementations.
- **Raid Level 10:** Uses both mirroring and striping to provide a higher degree of read and write performance than the other RAID levels, but it is more expensive because of the use of additional drives.

Remote Access Security

- **Remote Access Services (RAS)** are deployed using servers and software to allow remote workers the same access used by employees working at the physical organization's facility.
- Remote access policies should be built to provide consistency, should be part of a new user's training requirements for network use, and should be managed by the information security group within an organization.

Virtualization

- Virtualization allows system administrators the opportunity to consolidate system resources using a logical view of system resources rather than a physical environment.
- The instances of an operating system operating on a virtual machine are managed by what is called a hypervisor. The **hypervisor** controls the flow of data that includes instructions between the guest OS and all of the physical hardware.

Summary

- The operating system is the foundation of any application development endeavor.
- The most important aspect of new application development and the operating system is to design the application with the security available to you with the currently deployed operating systems in your organization.

In class exercises revisited

Bob's Pizza Shack

In groups consider this scenario and draw a rough system diagram and identify the OS concerns in the diagram and list your concerns

- Bob is a small business owner of Bob's Pizza Shack and wants to create a website to allow online credit card delivery orders
- What are Bob's security concerns from a network perspective?
  - Consider ones in own environment
  - Consider ones associated with the public facing web site
  - Consider data concerns

Alice's Online Bank

In groups consider this scenario and draw a rough system diagram and identify the OS concerns in the diagram and list your concerns

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns from a network perspective?
  - Consider ones in own environment
  - Consider ones interoperating with another bank
  - Consider ones interacting with customer
    - Web
    - Mobile app

Location based social media app

In groups consider this scenario and draw a rough system diagram and identify the OS concerns in the diagram and list your concerns

- Open source group wants to create a mobile app to allow groups to communicate/find each other in public demonstrations/protests
  - Communication internet, as well as, P2P (WiFi/Bluetooth) in case internet cut off – so if person you want to contact is on other side of crowd and no internet as long as P2P network can be established with app can reach somebody outside your immediate vicinity via the P2P network
  - Should be able to communicate securely messages and images to people you identify within your group (group as whole or direct)
  - Should be able to share GPS location with people in group (group as whole or direct)
- Broader scope – Who are potential threats and associated ways could attack/weaken system?