IT 609
Network and System Administration

Operating System Management

Tuesday September 21, 2021

Section Overview

- Operating System Management
- Assignment #01 - Part 1
- Quiz #02 - Data Centers, Performance, and VDI

End User Computing

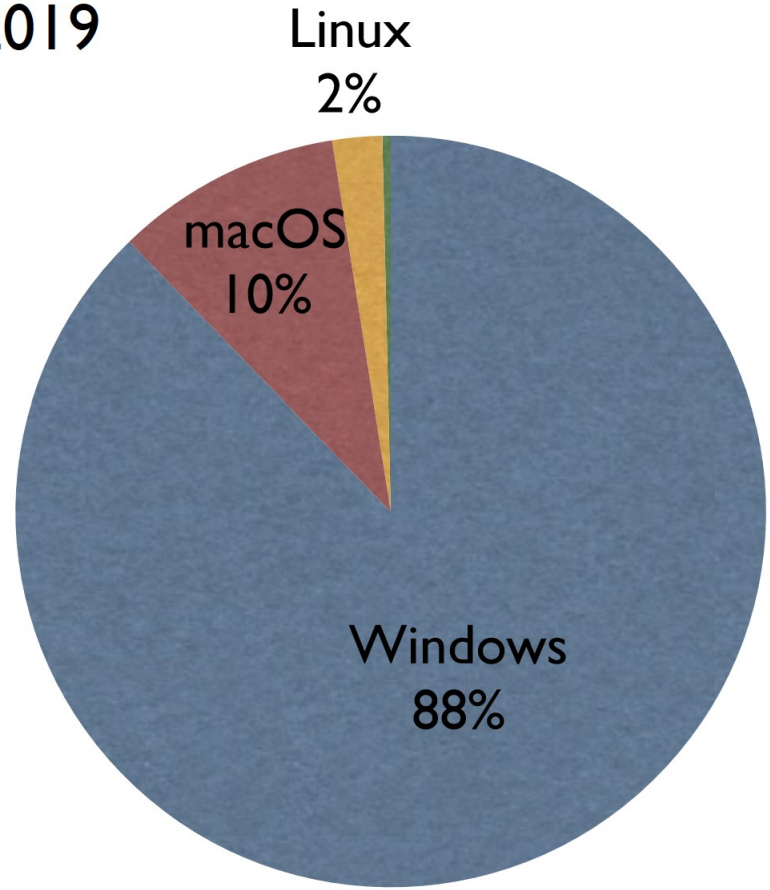
End User Computing

- Who is an “End User”?
- What are they using?
- How is this changing?
- What are issues and concerns about "End Users" and their devices?
- What do system administrators need to do?

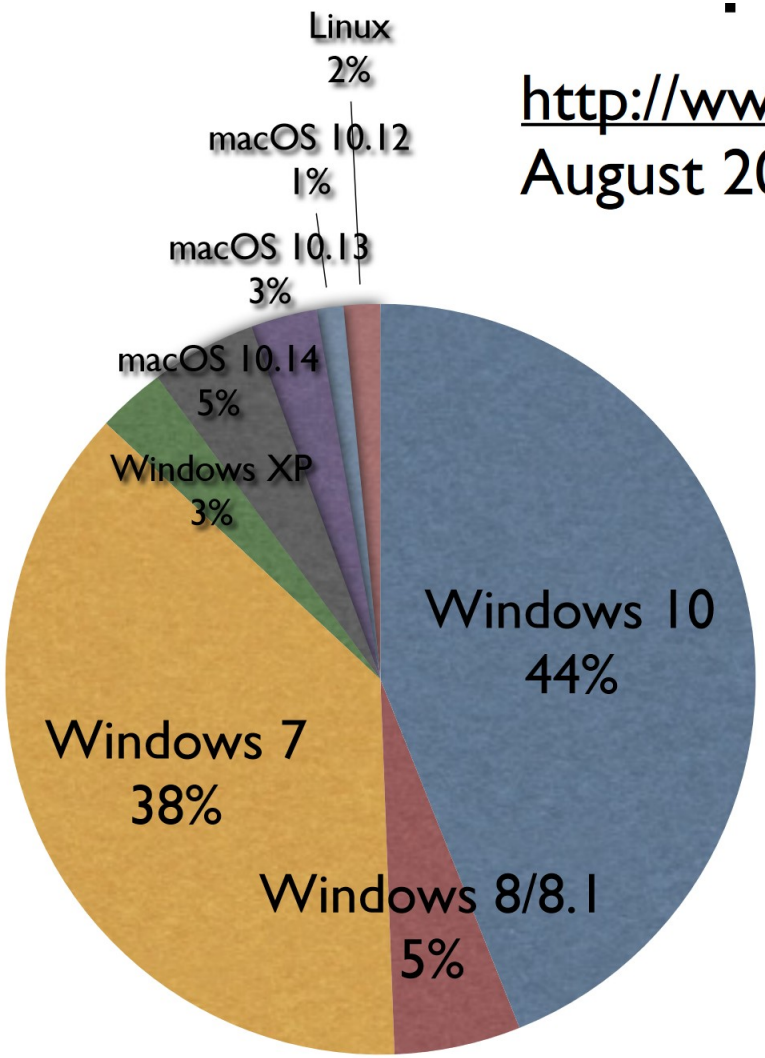
Desktop OS

http://www.netmarketshare.com

August 2019



Desktop OS

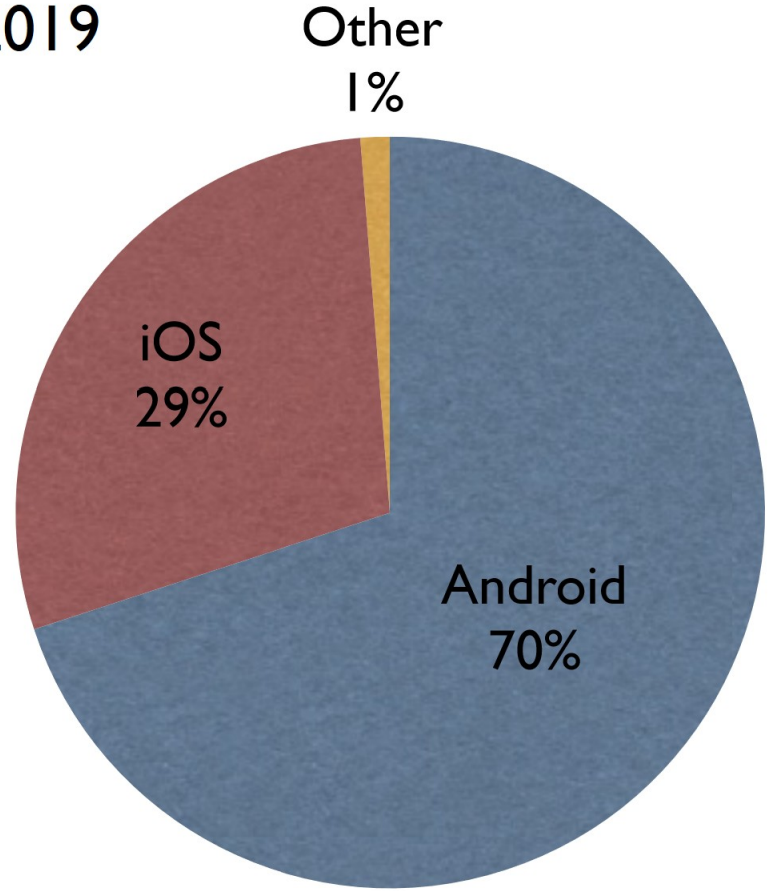


http://www.netmarketshare.com
August 2019

Mobile OS

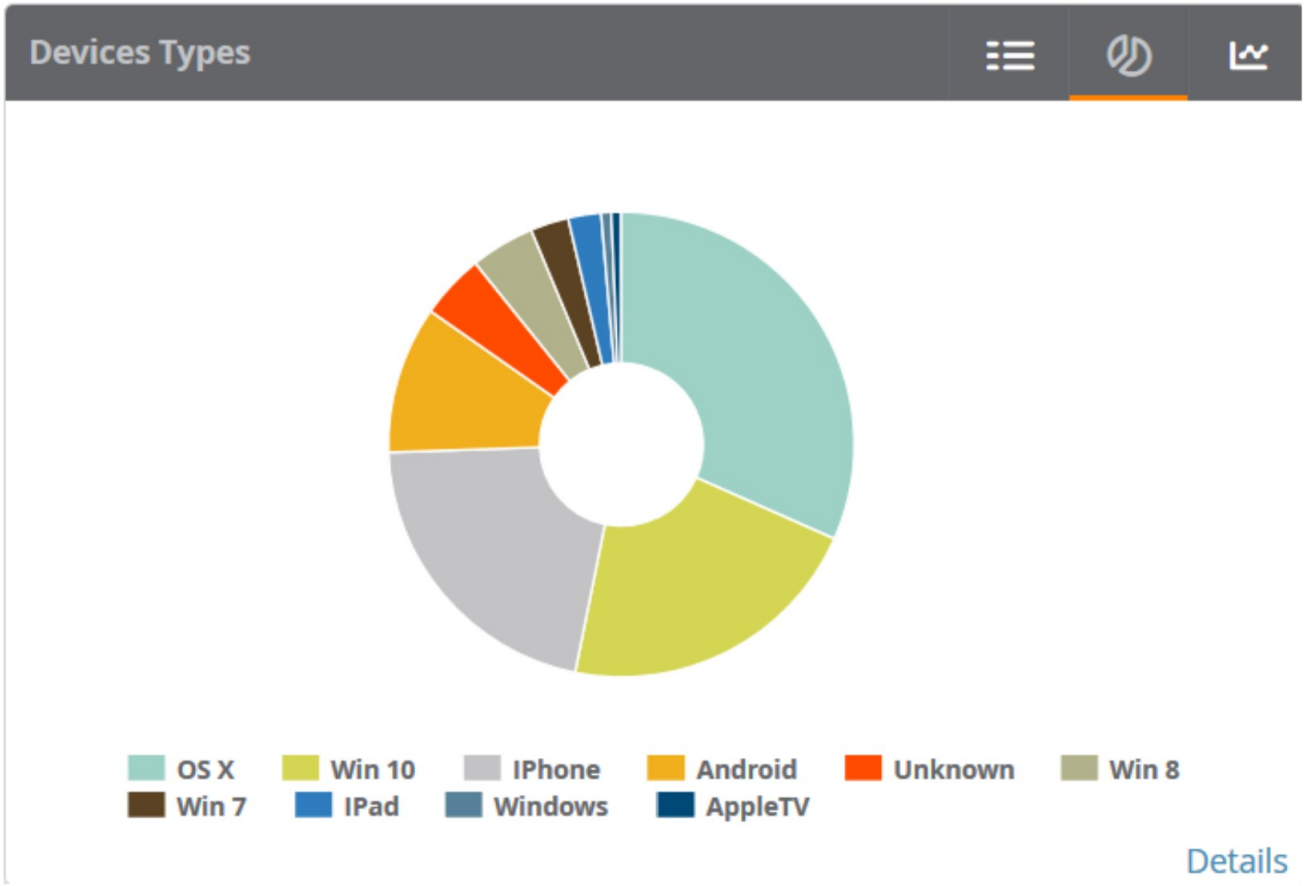
http://www.netmarketshare.com

August 2019



At UNH

UNH Network Operations, August 2016



The Market - Windows

Why?	90% of the market
Vendor	Microsoft
Platform	Desktops, laptops, tablets, servers
Current release	Windows 10 - 1903 (May 2019)
Release info	Windows 7 (Oct 2009), EOL Jan. 2020 Windows 10 first release (July 2015)
Server release	Windows Server 2019

The Market - macOS

Why?	Most widely deployed Unix-based OS, leader in user experience
Vendor	Apple
Platform	Mac desktops, Mac laptops
Current release	macOS Mojave 10.14
Release info	OS X 10.8 (July 2012) - 64 bit kernel macOS 10.15 (Fall 2019) - 64 bit apps
Server release	Not really…

The Market - Linux

Why?	Best known open source OS
Vendor	It's complicated (SuSE, Ubuntu, Fedora Core, Red Hat, CentOS, etc)
Platform	Anything
Current release	Linux Kernel 5.2 (July 2019)
Release info	Many different variants and distributions
Server release	Same as desktop or server-specific distributions

The Market – Android

Why?	Most widely used mobile OS
Vendor	Google
Platform	Phones, tablets, watches, etc
Current release	Android 9 Pie (August 2018)
Release info	Devices often lag behind official release, lots of versions in the wild

The Market - iOS

Why?	First modern mobile OS, 2nd in marketshare today
Vendor	Apple
Platform	iPhones, iPads (iPadOS), Apple Watch (watchOS), AppleTV (tvOS)
Current release	iOS 12 (Sept 2018)
Release info	Annual releases, rapid upgrade of devices

End User Concerns

- Easy to use - intuitive interface
- Reliable and Secure
- Power Management (Battery Life)
- Storage (Files)
- Networking
- Applications
- Customization

SysAdmin Concerns

- Installation
- Organization
- Reliable and Secure
- Monitoring
- Reporting

Computer Life Cycle

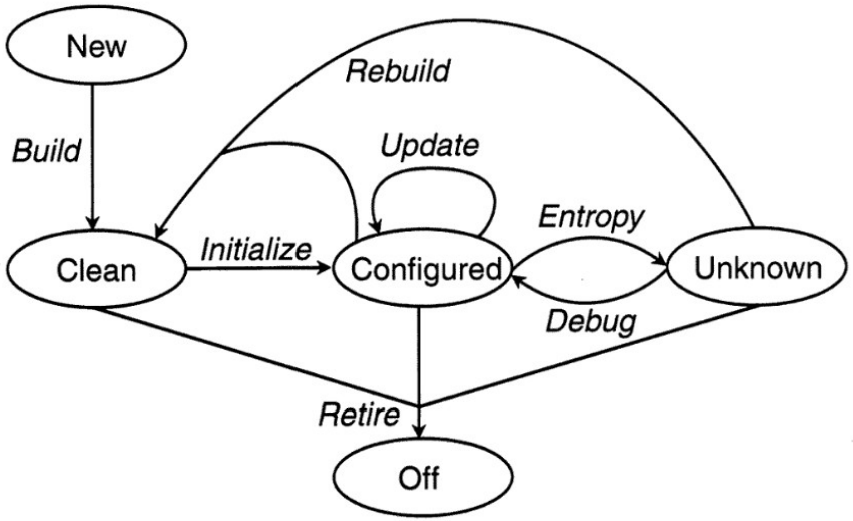


Figure 1.1: Evard's life cycle of a machine

Rémy Evard, 1997. "An Analysis of a Unix System Configuration"

Computer Life Cycle

- The goal of proper system administration is to keep the device in the “configured” state as long as possible.
- How do you get a device into that state quickly?
- How do you keep it from being affected by Entropy (i.e. keep in that state)?
- How do you handle the Update process?
- How do you efficiently repeat this for 100s or 1000s of devices?

Installation

- Generally, easy and straight forward now.
- Do not accept the defaults (without knowing the impact) and beware of what the vendor provides.
- Simplify, keep only what you really need.
- Not a lot of choices now - except maybe 32 versus 64 bit (though quickly going away as well).

Partitioning

- Single physical drives (or RAID arrays) can be partitioned into multiple logical disks.
- Can be adventageous to keep certain kinds of files or applications separate from the OS.
  - Reduces chance of corruption.
  - Simplify, backup strategy.
- Safer for Virtual Memory swap space (may be required, definitely a benefit).
- Could limit long run flexibility.

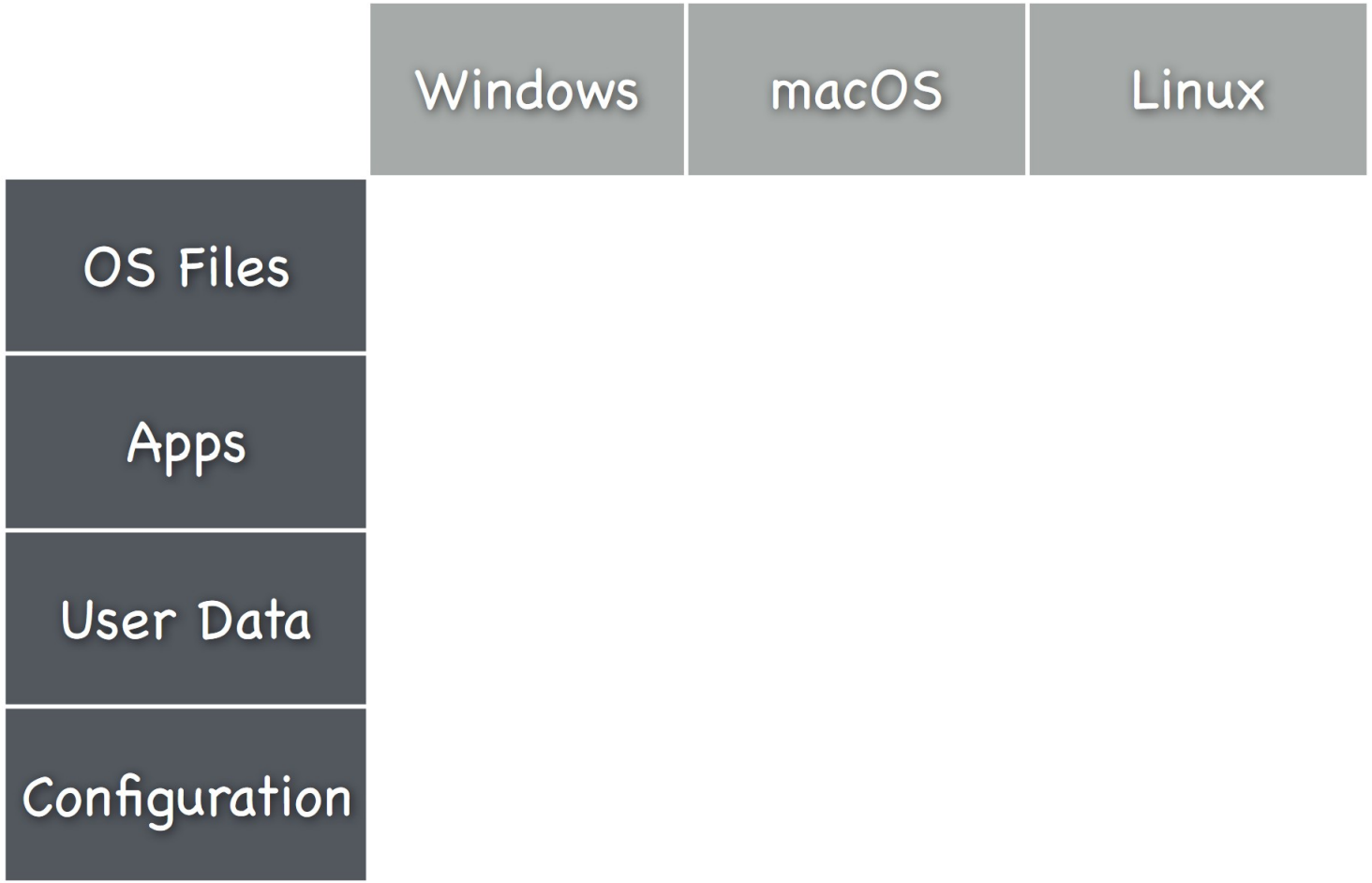
32-bit versus 64-bit

- A 32-bit process is limited to 4 GB of memory.
  - On Windows, for legacy reasons, 32-bit is normally limited to 2 GB per process.
  - Total memory includes video RAM, BIOS, and other overhead so often less than 4 GB is usable.
  - Simplify, backup strategy.
- This affects all operating systems.
  - Windows, Linux, macOS

32-bit versus 64-bit

- 64-bit is not inherently faster/better.
- 64-bit is a major benefit for processes that use larger than 4 (or 2) GB.
  - New limit is 8 TB!
- 64-bit OS can run most 32-bit applications if supported, but there can be issues with device drivers and other low-level processes.
- 64-bit apps only run on 64-bit capable OS.
- 64-bit apps cannot usually work with 32-bit add-ons or plug-ins

What Goes Where?



What Goes Where?

	Windows	macOS	Linux
OS Files	C:\Windows	/System /Library	Lots of places (/bin, /sbin, /lib, /etc, /var)
Apps	C:\Program Files C:\Programs Files (x86)	/Applications	/usr
User Data	C:\Users	/Users	/home
Configuration	Registry	Text files (various locations)	Text files (/etc)

File System Layout - Windows

`Users`

- User settings and file storage
- `Public` - items for everyone
- `Default` - used as the basis for individual profiles
- Contains User portion of Registry

`Program Files` (and `Program Files x86`)

- Some shared resources (Common Files, etc)

`Windows`

- `System` and `System32` hold most of OS files
- Registry files in `System32\config`

File System Layout - macOS

`/Applications` - OS X-native applications

`/Library`

- Fonts, plug-ins, 3rd party drivers, etc for all users
- Can only be modified by Administrators

`/System` - owned by root

- Operating system
- Library folder of standard resources

`/Users`

- Home directories
- Automatically subdivided

Also normal Unix directories hidden from users

File System Layout - Linux

/ - root file system, always required

bin - system binaries

sbin - binaries for system admin functions

lib - system libraries

etc - configuration files, startup scripts

dev - device files

proc - process and device information

var - logs, print spools, changeable items

mnt - mount points for CD, floppy, etc

home - user home directories

usr - user related programs (aka applications)

tmp - temporary files

File System Layout - Linux

/etc

- inittab - init level settings
- passwd & group - users and groups
- fstab - auto mount file systems
- lilo.conf - LILO configuration
- printcap - printer settings
- skel - default .files for new users
- rc.d - startup and shutdown scripts
  - rc.sysinit
  - rc.local
  - rc.initd

File System Layout - Linux

`/home`

One directory per user

Might have special directories for web or ftp

Often a separate disk partition on larger, shared systems

File System Layout - Linux

`/usr`

- Also often a separate file system
- Contains `bin`, `lib`, `local`, `share`, `doc`, & others
- Actual end-user applications wind up here
- `/usr/X11R6` - X Windows system

What Goes Where?

- Why does this matter?
- Keep OS, applications, and users' file(s) separate.
- Makes for easier backup, support, and maintenance.
- Provides for easier, cleaner security of OS and application files as well as multiple users' home directories.
- Allows for a permissions model where normal users can read, but not modify the OS, apps, and others users' data.

What Goes Where - Mobile?

- You don’t get a choice!
- Normally no direct file system access.
- “App Store” for software installations.
- Underneath, though, there’s Unix down there...

Security

- What's being secured and why?
  - Integrity and availability of the operating system, applications, and configuration.
  - Confidentiality, availability, and integrity of personal data
- How?
  - User identity with grouping.
  - File-level permissions.
  - Special protections for OS files.

OS Security - Users

	Windows	macOS	Linux
User ID	Security Identifier (SID) S-1-5-21-3623811015-3361044348-30300820-1013	User ID (UID) 501 to start	User ID (UID) start varies
Important identities	Administrator System	0 = root disabled by default	0 = root
Important Groups	Administrators Users	Administrator (admin, wheel) Standard (staff)	wheel

OS Security - Files

	Windows	macOS	Linux
File Security	Access Control Lists (ACLs) Full Control, Modify, Read & execute, list folder contents, Read, Write	Unix Read, Write, eXecute for owner, group, and all plus ACLs	Unix Read, Write, eXecute for owner, group, and all
How applied?	Administrators can modify C:\Windows; C:\Program Files; Users can read & execute only	Administrators can modify Library and Applications; Standard cannot	It's complicated, but normal users can only RX OS files and apps

OS Security - Extras

	Windows	macOS	Linux
OS protection	User Access Control (UAC) - prompt for confirmation of admin tasks	System Integrity Protection - No modification of core OS files and pre-installed apps even by root; Prompt for some admin tasks; Packages	None generally; Security Enhanced Linux (SELinux) is an option
Elevate privileges	Right-click and "Run as Administrator"	sudo	sudo

Security – Common Themes

- Ways to restrict read & write access to individual files and directories
- Administrator vs. normal user access
  - Normal users cannot modify the OS, system-wide applications, etc.
  - Administrators have high level privileges – a security risk!
- Standard setups designed to not give unneeded access to files & directories
- Hiding or otherwise protecting core OS files is a good idea in addition to having them be read-only

Configuration

	Windows	macOS	Linux
GUI	Settings - newer Control Panel - legacy	System Preferences	Various GUI control centers exist, varies by distribution
CLI	"reg" command; PowerShell	"defaults" and other commands; direct text editing	direct text editing
Where?	Registry	.plist files - XML; other text files	Various text files; no firm standards

Windows - Registry

A unified repository for configuration and preference information

Replaces old system of many separate `.ini` files

Editing via `regedit`

Can be accessed over a network

Security privileges apply to particular branches or sub-trees

Registry values can be read and set via APIs as well as by exporting/importing Registry files (`.reg`)

Registry Organization

Two major sections:

- Machine data
- User data

Items that apply to the whole computer and all users are in the Machine sections

Personal settings are in the User areas

Standard permissions model means that administrators can modify most of both of these while normal users can only modify their User section

Windows – Registry Hives

HKEY_CLASSES_ROOT

Link to `HKLM\Software\Classes`

File types, extension mapping, resources

HKEY_CURRENT_USER

Link to `HKU\`<CurrentUserSID>

HKEY_USERS (`HKU`)

`.DEFAULT` - minimal user settings/prefs

HKU/<SID> - user preferences and settings, stored in Documents and Settings

Only portion of Registry that members of the Users group can modify

Windows – Registry Hives

HKEY_LOCAL_MACHINE (HKLM)

- Hardware - created at each boot
- SAM - Security Access Manager
- Security - more security settings
- Software - software configuration for all users
- System - hardware, device drivers, etc.

HKEY_CURRENT_CONFIG

Link to HKLM\System\CurrentControlSet\Hardware Profiles\Current

What's The Right Way

Best practices for OS setup and management are sometimes confusing and conflicting

Good sources:

- The OS vendor
- Security groups like CIS and SANS

Companies and government organizations may have specifically defined practices

- DOD - STIGs

Monitoring & Logs

Log data is only as useful as the OS and application programmers make them!

System admins can use logs in different ways

- Good
  - Review log files when anything "bad" happens
- Better
  - Periodically check log files for anything abnormal
- Best
  - Automated system to check log files for you and report errors or suspicious activity

Monitoring & Logs

Windows

- Event Log Service - Application, Security, System, & others
- Accessed through Event Viewer
- Can also turn on auditing of file access, etc

macOS & Linux

- `syslogd` - system log daemon
- Configured in `/etc/syslog.conf`
- Writes to various files in `/var/log`
- Security related items in `/var/log/secure.log`

Mobile Challenges

Multiple platforms

Locked operating systems

Configuration

App Stores

Lost devices

BYOD

It's mobile

It just isn't like Windows!!!!!!

Mobile Device Management

- Centralized control and management
- Deployment of standard setups to corporate devices
- On-demand enrollment of BYOD
- Over-the-air control
  - Configure settings
  - Deploy or remove applications
  - Enforce update installation
- Lost device security
  - Location reporting
  - Remote lock and wipe

Homework Assignment

- Get on to Discord
- Assignment #01 - Hardware Specification