Windows 10 and macOS Architecture

Benjamin Brewster

Why You Need to Care

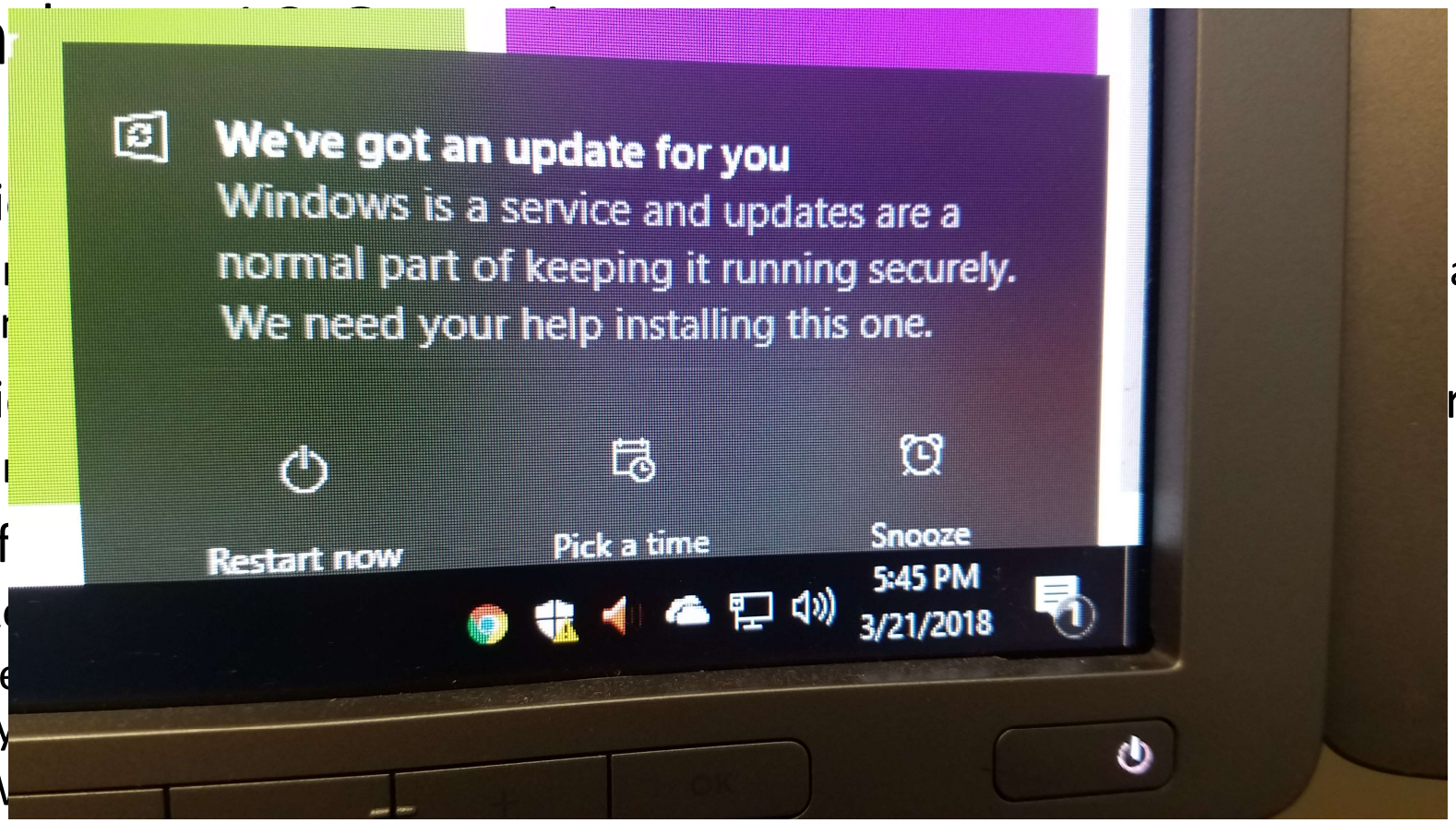
- Because someday you'll have to:
  - Reinstall Windows for the umpteenth time
  - Do *something* about that old Mac your grandma has
  - Know where to go to fix Windows printer issues
  - Examine the running processes and learn how to kill exactly the right one
  - Get under the hood with these OSs and configure them

Windows 10 Overview

- Editions *you* can buy: Home, Pro
  - Prices: $80-200 depending on Home versus Pro, OEM, retail versus download, and the market
- Editions *you* can't buy: Enterprise, Education, Mobile, at least 7 more
  - Prices: LOL
- Brief history/notes:
  - Released on July 29, 2015
  - Features Universal Apps that run on PCs, tablets, smartphones, embedded systems, Xbox One, Surface Hub and AR devices
  - Windows Updates cannot be disabled
  - Twice-yearly (Spring, Fall) updates that add major new features; think SaaS

Win

- Editi
  - Pr
    ar
- Editi
  - Pr
- Brief
  - Re
  - Fe
    sy
  - W
  - Twice-yearly (Spring, Fall) updates that add major new features; think SaaS



ad,

re

Windows 10 Architecture Overview and Detail

Important Programs in Windows 10

- We can gain information about what Windows is doing by examining what is running
- Task Manager can view all kinds of things, but limits our ability to see the actual underlying processes

- Way better is Process Explorer:
  - https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer

Important Programs in Windows 10

Say	Demonstrate
• Lack of specificity, though breadth is nice	• Task Manager tabs
• The rest of these are shown in Process Explorer	• Process Explorer: File->Show Processes for All Users
• The kernel	• System
• Handles shutdown, consoles, and other Win32 tasks	• Client Runtime Subsystem: csrss.exe (x2)
• First process started by kernel, manages environment variables, starts Win32 subsystem, starts virtual memory, starts winlogon.exe	• Session Manager Subsystem: System -> smss.exe
• Runs processes at system boot for all logons	• Wininit: wininit.exe
• The login process	• Winlogon: winlogon.exe
• Manages all services	• Service Control Manager: wininit.exe->services.exe
• Holds a particular service process	• Service Host: winint.exe->services.exe->svchost.exe
• Renders the visual UI	• Desktop Window Manager (DWM): winlogon.exe->dwm.exe
• Manages user-started programs and file browser(s)	• Windows Explorer: explorer.exe

Important Services in Windows 10

Say

- The paths in Process Explorer aren't all that useful: use Task Manager instead to see what's running

Demonstrate

- Process Explorer Service command line entries
- Show Service entries in Task Manager on Processes tab
- On Services tab, stop and start "Spooler", the print spooler

The Windows SysAdmin Shortcut Menu

Say

- Shows the basic hardware installed, System Type (32 or 64 bit), NETBIOS name, and installed OS version
- Quick access to the most important Windows sysadmin tools!
  - Task Scheduler (more on this another day)
  - Event Viewer (automated processing demo another day)
  - Shared Folders
  - Performance
  - Device Manager
  - Disk Management
  - Services

Demonstrate

- WIN+X
- ->System
- ->Computer Management
  - Briefly show each component
- Tour of Disk Management layout

Installing Software on Windows 10

Say	Demonstrate
• The Program Files themselves are written to either “Program Files” for 64-bit software, or “Program Files (x86)” for 32-bit software. These are protected folders, so normally software doesn’t write settings or other data frequently to them after installation	• Program Files & Program Files (x86)
• Used for non-user-specific application data	• ProgramData
• User-specific application data that follows the user on a domain	• C:\Users\<USER>\AppData\Roaming
• User & machine-specific application data	• C:\Users\<USER>\AppData\Local & …\LocalLow
• Stores machine-specific settings and config data for the software	• Registry (via regedit)
• Some games like to write data to the users documents folder to make it easy to find and backup	• The users Documents folder

Installing Software on Windows 10

Say

- Programs are typically installed as either:
  - .EXE executables that manually copy files to the appropriate places, write registry values, and configure shortcuts and environment variables to enable starting the program
  - .MSI files, which are packaged programs that use the Windows Installer APIs to do the same installation tasks
- Programs can be removed from the "Apps & features" area in Settings
- The Uninstall and other management features in here use the Windows Installer tool to do their work

Demonstrate

- WIN+X -> Settings -> Apps (Loads Apps & Features)

Important Folders and Files in Windows

Say	Demonstrate
Main storage location for Windows, mostly contains other folders and a few key apps (regedit.exe, etc.)	C:\Windows
Used in old 16-bit Windows editions, empty now	C:\Windows\System
Most of 64-bit Windows itself	C:\Windows\System32
32-bit Windows files	C:\Windows\SysWOW64
Non-user-specific temporary files	C:\Windows\Temp
Location of system-specific Registry files	C:\Windows\System32\Config
User-specific portion of Registry	C:\Users\<USER>NTUSER.DAT
Where print jobs sit until finished - delete this to free stuck print jobs!	C:\Windows\System32\spool\PRINTERS & ..\SERVERS
Virtual Memory page file	C:\pagefile.sys
System Restore points, search index databases, Volume Shadow Copy entries	<DRIVE>:\System Volume Information

Installing Windows on a New VM

- Broad strokes (this is a homework assignment to go play with):
  - Create VM in VirtualBox
    - For Windows 10 64-bit, I recommend assigning two CPUs, 2 GB RAM, all the video RAM, and a fixed disk size of at least 16GB
  - Insert the Windows 10 .ISO into the VM so that the VM boots off of it
    - Settings -> Storage -> Select the CD drive -> click the little CD icon on the far right
  - Start the VM
  - You'll want to create a "New" partition when Windows asks you to
  - You'll probably need to Eject the .ISO after Windows does the initial install, or it'll just boot off of it again when it reboots (don't "Remove Attachment" - that removes the actual/virtual CD drive)
- It's very easy, plus the correct drivers are all pre-loaded for the VM

Driver Installation Order

- If you were installing Windows yourself, on bare hardware, you'd install the drivers in this order:
  - **MOBO**, sometimes called Firmware; includes CPU
  - **BIOS**, if needed
  - **Storage** controllers and/or management software for RAID arrays, SANs, etc.
  - **GPU**, if not built-in to the MOBO
  - **Network**, if needed (this is often part of the MOBO drivers these days)
  - **Audio**, if needed (this is often part of the MOBO drivers these days)
  - **Optical** disk drives, if needed
  - **Input**, like special gaming mice and keyboards, if needed
  - **External**, like printers, webcams, other external USB devices

Critical Things to Configure in Windows

Say	Demonstrate
• This is how your PC is found on the network locally	• Assign new NETBIOS name, reboot • WINX -> System -> Rename…

• Make these changes from the common defaults	• View -> Options -> Folder Options -> View tab
	  • Check “Always show menus”
	  • Check “Show hidden files…”
	  • Uncheck “Hide extensions for known file types”
	  • Uncheck “Hide protected operating system files…”
	  • Uncheck “Use Sharing Wizard”

Windows Updates

Say

- Windows isn't as buggy as you might think: the problem is normally one that exists with buggy third-party software
- New bugs that affect usability and security are constantly discovered
- System Updates fix these bugs, though knowledge of the existence of the bugs can cause "zero-day" viruses that exploit the bug until the patch hits all systems
- In the past, Windows updates could be disabled, but not anymore
  - Yeah people are mad, but this is better than botnets

Demonstrate

- WIN+X -> Settings -> Update & Security
- Explore "Change active hours", "Restart options", and "Advanced options"
- Note how there is no "disable" button!

macOS Architecture Overview

- Mach kernel
  - A microkernel
- BSD subsystems
  - BSD is a fork of UNIX; includes basic binaries like `ls`, `cat`, etc.
- Together, the core of macOS is called Darwin, which is shared with iOS, tvOS, and watchOS
- Apple GUIs (Aqua) and APIs (Cocoa, etc.)

Installing macOS

- This isn't NEAR as common as it is in Windows
- Normally, you'd just do one of the following:
  - Stick in the DVD and reformat (harder to do these days since there's no ODD)
  - Apply the update from the App Store to upgrade
  - Hold Command+R to boot into a "macOS Utilities" menu where the OS can be reinstalled and the partitions formatted
- But if you're doing it on a VM:
  - https://www.howtogeek.com/289594/how-to-install-macos-sierra-in-virtualbox-on-windows-10/
  - iTunes, Facetime, other Apple-authored software won't work
- Since Apple builds the hardware (is this good or bad?), there aren't separate drivers to install

macOS Disk Management

Say	Demonstrate
• Like in Windows, the general, easy to find System Preferences is not where administration really happens	• Apple -> System Preferences
• System Information gives you specifics about your hardware	• Finder -> Go -> Utilities • ->System Information
• The Built-in Disk Utility won't show you all the partitions in the system	• ->Disk Utility
• Fire up the terminal to see all the disk partitions	• ->Terminal • `$ diskutil list`
• You can do all the normal commands from here or Disk Utility	• `$ diskutil reformat`

Installing Software onto macOS

Say	Demonstrate
	• Double click .dmg on desktop
• Typically downloads are .dmg files, which are Apple Disk Image files that contain compressed data which is mounted as a new volume	• Show in Disk Utility the mounted image
• Once mounted, the data can be copied off of it	• Eject by moving to trash
• When these folders contain programs to install, you simply drag them to the Applications folder	
• Uninstallation is just dragging them from Applications to Trash	• Finder -> Go -> Applications
• Some Applications come as .pkg files, which use the Apple installer in the same way that the Windows Installer works	

Other macOS Folders

Say

- In general, this is simpler than Windows and Linux
- Where these personal folders are actually located
- You can see the Applications folder here
- /Volumes has the mount drives
- ~/System/Library and /Library and ~/Library has base settings, computer-wide mods to those settings, and user-specific mods to those settings
- /System and /Network are for admins to play in
- The rest of the lower-case folders we'll see in the Linux overview

Demonstrate

- Finder -> Go -> Terminal
- $ ls -pla (from ~)
- $ cd /
- $ ls -pla
- $ ls -pla /Users/macuser
- $ ls -pla /Applications
- $ ls -pla /Volumes

macOS Updates

Say

- You can see what updates are automatically being applied in the standard App Store
- Disable updates in the preferences
  - I've done that in our VM so that it doesn't spend its limited CPU time trying to download a bunch of updates
  - Note that in a VM, several patches will fail to install, like iTunes, Facetime, etc.

Demonstrate

- Apple -> About This Mac -> Software Update
- App Store -> Preferences

Command Line Interface

- Both Windows and Apple have extensive CLIs with a long history behind them.
- Windows 10's DOS is supplemented now with PowerShell and bash
- macOS uses bash on BSD

- Important, powerful, dangerous, yet infrequently used tools and options are only available in the CLI on both OSs

Conclusion

- All Operating Systems consist of collections of files
- Messing with those files causes things to stop working
- If you know what you're doing, you might be able to fix certain things
- But in bad events, you have to recover from a known good system (recovery partitions, OS repair from DVD, etc.)
- In really bad events, the OS can "simply" be reinstalled, often with the loss of all of your kid's baby pictures