Securing the Operating System: Digital Signatures, OS Vendor Certification, and the impact on Open Source Software

Jeffrey Altman and Daria Phoebe Brashear
Your File System Inc.
2015 AFS and Kerberos Best Practices Workshop

App Models and Quality Control

What is an App Model

- An application model specifies the rules by which an application is installed, executed, upgraded, and uninstalled
- The “holy grail” for end users is an App Model that permits applications to be installed, executed, upgraded and uninstalled such that the OS state at the beginning matches that at the end

App Model examples

- iOS
- Windows Metro/Modern and AppX
- Google Play

Applications implemented to the specifications of these app models are “zero footprint”.

App Stores and the Consumer Experience

- The iP* devices are consumer devices not computer professional devices
- No system administrator required
- They must be as safe and easy to use as a “toaster”

- The Genius Bar is genius because it permits Apple to sell a consumer device that wasn’t yet consumer safe

The Windows Experience

- From the moment the OS is booted and the first upgrades are applied the performance of the OS begins to degrade
- Every application, assembly, service and driver installation grows and fragments the registry and the \WINDOWS directory
- The Windows 10 AppX model is an attempt to fix that by sandboxing “full trust” apps

Kernel drivers and System Stability

- Kernel drivers, modules or extensions all execute at Ring-0 of the processor
- They have full control over the system without bounds
- Minor coding errors can “panic” or “Blue screen of death” a system
- The mistakes of third party vendors damage the “OS Brand” reputation

Malware and Reputation

- The existence of malware and the distribution of modified versions of “trusted” applications harms the reputation of the OS and the App vendors
- Decreased reliability increases end user frustrations and reduces the market size for products and services

OS X

OSX – Why Sign?

- gatekeeper
  - running binaries
- application firewall
  - using network resources
- kexts
  - ability to extend kernel functionality
- installer
  - ability to install packages

OSX – Sign What?

- Installers
- Scripts
- Binaries
- Libraries
- Kernel extensions
- Plugins

OSX – Sign How?

- With a Distribution Certificate issued by Apple
  - A separate developer cert is used before distributing, if desired
- With one endorsed for “kexts” if signing a kernel extension is required

OSX – Sign Why?

- To prevent malicious code from being
  - Installed via Installer
  - Run by the user
  - Loaded into the kernel by an admin
  - Loaded into another process via dylib

OSX – Issues!!!!

- Certificates only from Apple
  - But Apple does not certify content after signing, unless for App Store
- App Store does not allow kexts
- “kext” certificates not issued to all comers
- Fussiness with “kext” signing
  - The means to do so has changed in each version, slightly
- Issues from Application Firewall
  - And a little footnote on how Application Firewall works

Windows 10 and Server 2016

Windows App Installation Formats

- InstallShield
- Nullsoft
- MSI

- None of these installation processes define an “application model”. Any application to be distributed via the Store must adhere to the AppX model

New formats for Windows 10

- AppX
  - Userland application processes
  - Bundled assemblies
- Windows Update
  - Driver installation
- MSI (cannot be used on Nano)
  - Network Providers
  - Explorer Shell Extensions
  - NT Services
  - Side by Side Assemblies

Microsoft responds to the NSA

- The “Snowden” revelations that the NSA accessed private data within and between internal Google, Yahoo and Microsoft data centers hurt business outside the U.S.
- To rebuild trust, Microsoft wants to ensure that “evil” code cannot be loaded in Azure
  - Same security level for internal corporate data centers

Microsoft will sign all drivers

- Too many vendors have had their infrastructure breached and their valid certificates used to sign “malware”
- Kernel drivers have full control and must be fully trusted
- Microsoft will ensure there is an audit log of all signed drivers and now be able to revoke particular signatures (if necessary)
  - This also permits MSFT to use proprietary signing algorithms

YourFileSystem

Device Guard

- The OS is now split into two hypervisor guests
  - A readonly VM that verifies all signatures and enforces policy (Device Guard)
  - A readwrite VM that is the user facing OS
- No driver or executable module can be loaded in the readwrite VM without approval of the Device Guard VM
- Device Guard builds upon Secure Boot and Trusted Platform Modules

Certification

- Certification of each driver build is required for Server 2016 deployment
- The Microsoft signature will indicate which OS releases a driver is certified for
- Device Guard will not permit a driver to be installed on a Server OS that is not in the list

Quality Control

- Certification
  - is not a security mechanism
  - It is a quality control mechanism
- Certified applications and drivers can be trusted by end users to provide a consistent experience and be heavily tested

The Costs

- Microsoft charges no money to certify and sign drivers or applications
- However the certification requirements raise the bar for developers which in turn will impose significant indirect costs
  - New mandatory features
  - Static analysis tools
  - Mandatory use of the latest Microsoft compilers
  - Continuous QA Testing
  - Mandatory integration with Windows Error Reporting and Analysis

Conclusions

Broader Trust might increase adoption by Enterprise

- Enterprises are very cautious about deploying kernel extensions or drivers
- Most want certification which has never been available before
- Most want the OS vendor to bless the code

The Downsides

- Significantly increased overhead
  - Prevents students and other individuals from learning through experimentation
  - Smaller pool of skilled developers
- Non-corporate and unfunded entities will find it increasingly difficult to participate in this space

To some extent that is by design, to some extent it is an unwanted side effect

Questions! Answers?

YourFileSystem

255 W 94TH ST
New York NY 10025 USA
+1 212 769-9018
sales@your-file-system.com
http://www.your-file-system.com