Playing In The App Sandbox

Boisy G. Pitre
@boisypitre

MACTECH CONFERENCE 2012

TEE-BOY

About Me

Senior Software Engineer at NUANCE

Developer of WeatherSnoop

Co-author of *Developer to Developer* monthly column in MACTECH Magazine


Presentation Goals

- Examine App Sandboxing's "Raison d'Etre"
- Peek at the Technology Behind Sandboxing
- Explore Entitlements and XPC
- Demo
- Dirty Little Secrets!

What Is App Sandboxing?

- An "Electric Fence"
- Has roots in iOS
- Keeps the app honest
- A preemptive strike by Apple to head off malware and strengthens platform





Keeps “Bad Actors” Out



MACTECH CONFERENCE 2012

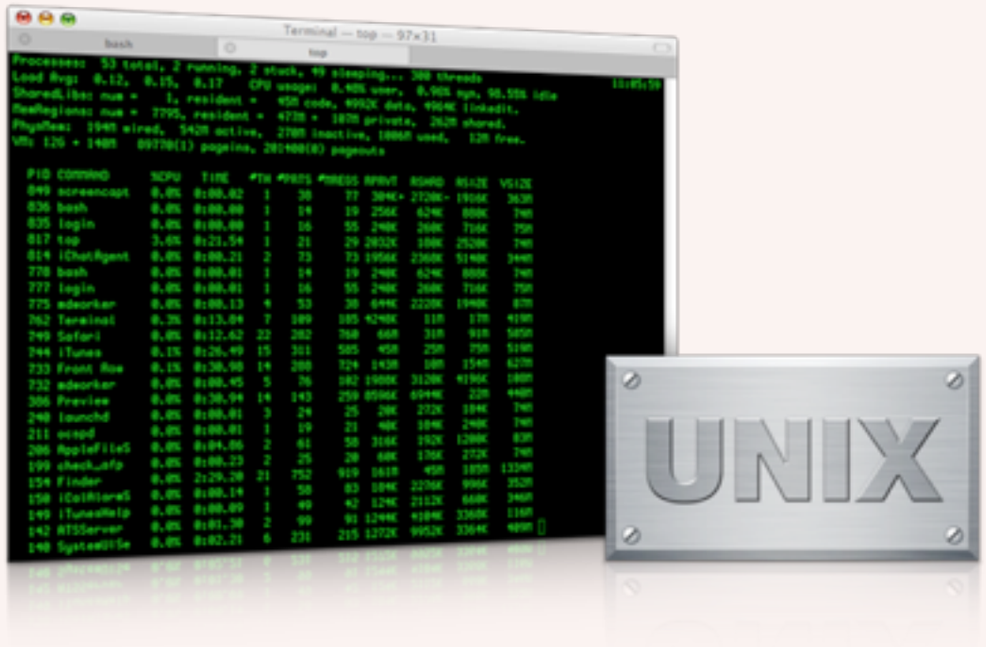

Why Sandboxing?

After all, isn't the Mac already secure??

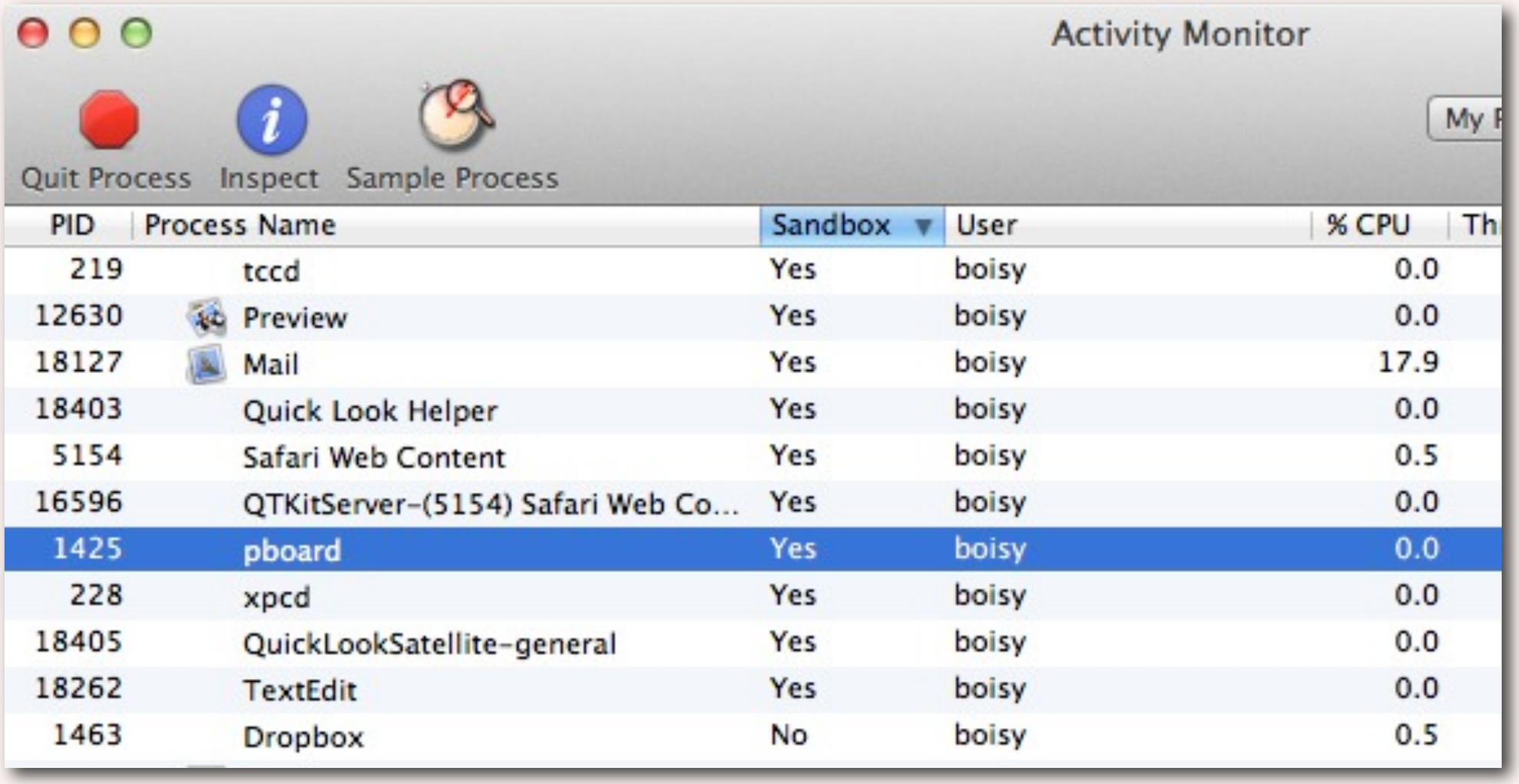
- It's good security practice
- Mac App Store requires it
- It's the Future...

Traditional UNIX Security

- Users and Groups
- File Permissions
- Access Control Lists

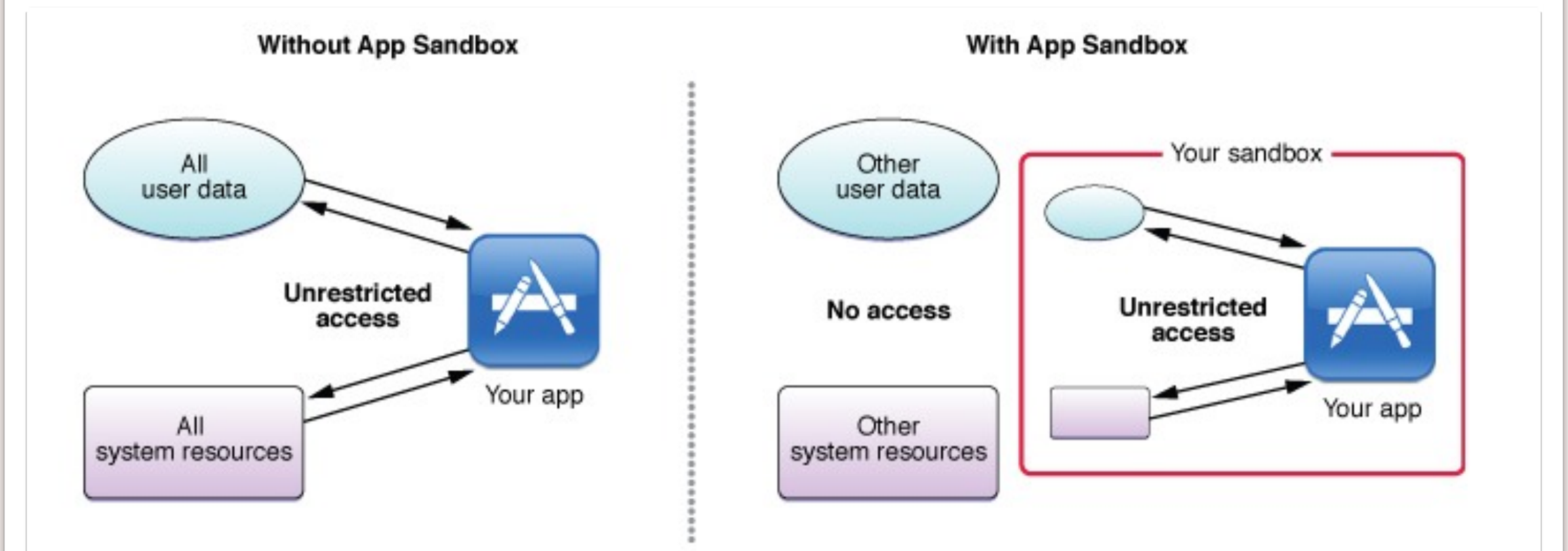


Sandboxed Apps



PID	Process Name	Sandbox	User	% CPU	Th
219	tccd	Yes	boisy	0.0	
12630	Preview	Yes	boisy	0.0	
18127	Mail	Yes	boisy	17.9	
18403	Quick Look Helper	Yes	boisy	0.0	
5154	Safari Web Content	Yes	boisy	0.5	
16596	QTKitServer-(5154) Safari Web Co...	Yes	boisy	0.0	
1425	pboard	Yes	boisy	0.0	
228	xpcd	Yes	boisy	0.0	
18405	QuickLookSatellite-general	Yes	boisy	0.0	
18262	TextEdit	Yes	boisy	0.0	
1463	Dropbox	No	boisy	0.5	

How Sandboxing Works



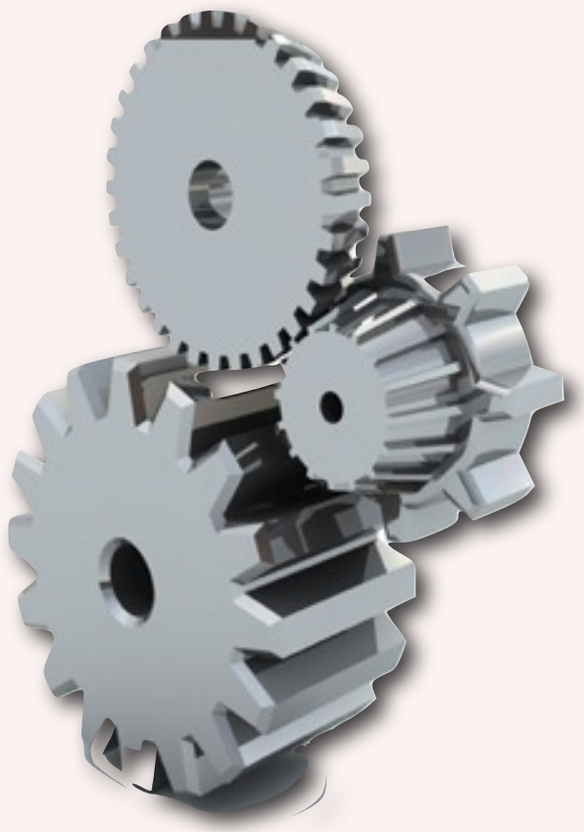
Who Can't Play in the Sandbox

- Kernel extensions
- Apps that set preferences of other apps
- Apps that send Apple events to other apps

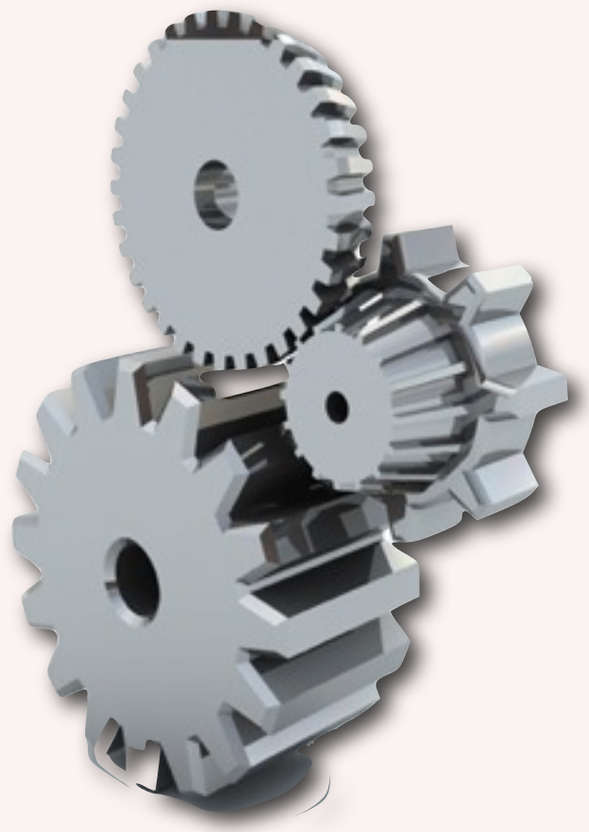
Sandbox? or Quicksand?

Delays In Enforcement

- Was coming November 2011
- Then Postponed to March 2012
- Again Postponed to June 2012
- Now: Mandatory for the Mac App Store
- NOT Required for non-MAS Apps (yet?)



Technology



Sandboxing's Vintage

Arrived in Mac OS X 10.5

Required for Mac App Store
for Mac OS X 10.6

Baked into the OS and is
here to stay!

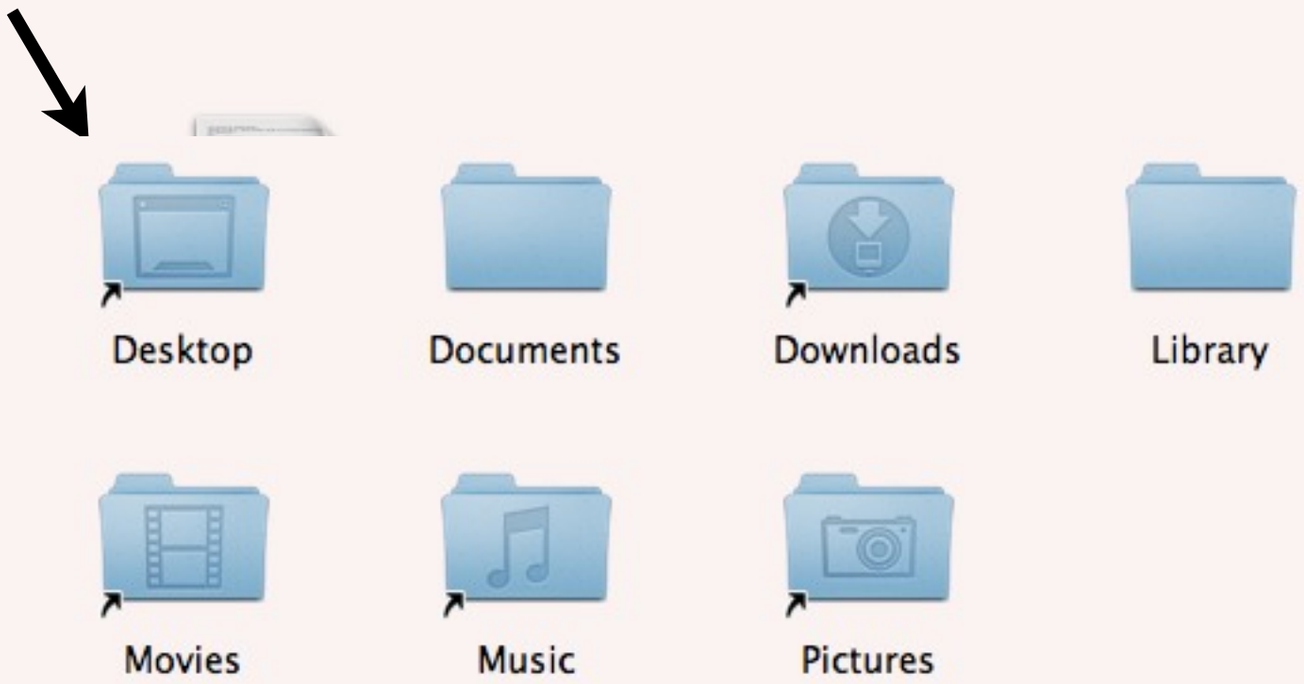
Under The Covers

- sandbox-exec
  - launches apps in a sandboxed environment
  - uses a profile to determine restrictions
  - /usr/share/sandbox
- sandboxd
  - daemon that performs sandbox services

Containers

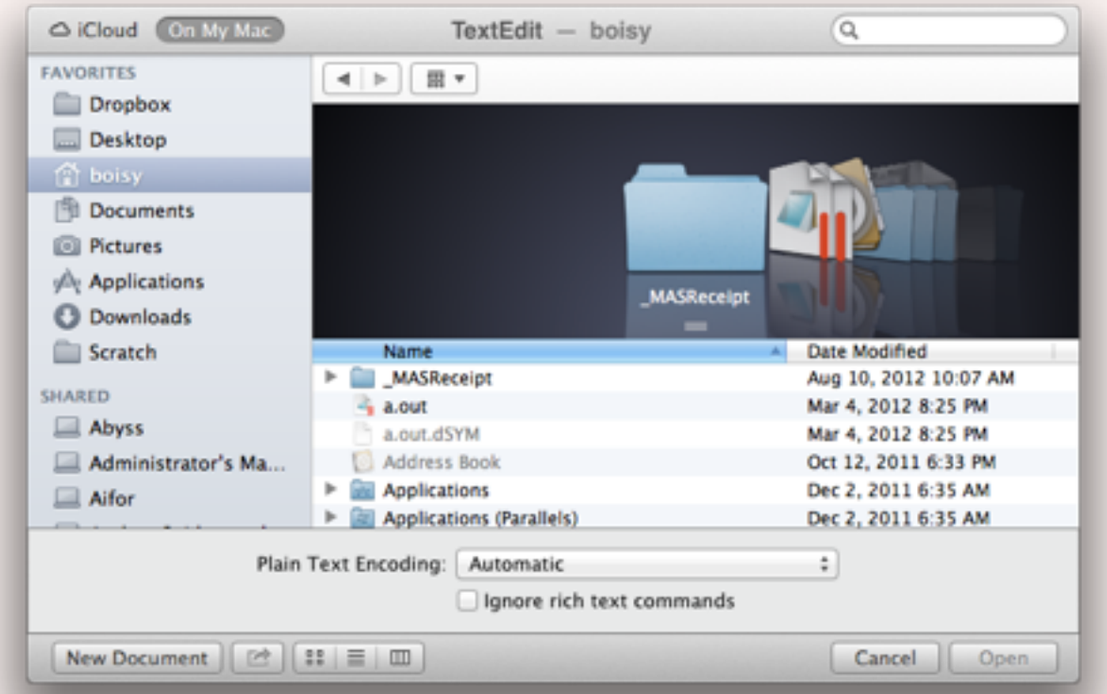
- Sandboxed apps get their own private file system
  - ${Home}/Library/Containers/<app_bundle_id>/Data/
- Access is unhampered in that folder

Container View



Powerbox (pboxd)

- Allows access to files outside of the container
- Supports NSOpenPanel, NSSavePanel, dragging to Dock icon
- User-directed, automatically makes selected files accessible for the duration of the application's run



Entitlements

Entitlements Are...

- "Grants" from Apple which allow your app to do certain things
- Specifically named (com.apple.security....)
- Enumerated in YourApp.entitlements plist file, used when signing your app

Enforcement

- Enforced at the system level
- Violations are flagged and prevented from executing
- Violations also show up in Console.app

Entitlements

Read-only access to the user's Movies folder and iTunes movies	`com.apple.security.assets.movies.read-only`
Read/write access to the user's Movies folder and iTunes movies	`com.apple.security.assets.movies.read-write`
Read-only access to the user's Music folder	`com.apple.security.assets.music.read-write`
Read/write access to the user's Music folder	`com.apple.security.assets.pictures.read-only`
Read-only access to the user's Pictures folder	`com.apple.security.assets.pictures.read-only`
Read/write access to the user's Pictures folder	`com.apple.security.assets.pictures.read-write`
Interaction with Bluetooth devices	`com.apple.security.device.bluetooth`
Capture of movies and still images using the built-in camera, if available	`com.apple.security.device.camera`

Entitlements

Recording of audio using the built-in microphone, if available, along with access to audio input using any Core Audio API that supports audio input	`com.apple.security.device.microphone`
Interaction with serial devices	`com.apple.security.device.serial`
Interaction with USB devices, including HID devices such as joysticks	`com.apple.security.device.usb`
Read/write access to the user's Downloads folder	`com.apple.security.files.downloads.read-write`
Use of app-scoped bookmarks and URLs	`com.apple.security.files.bookmarks.app-scope`
Use of document-scoped bookmarks and URLs	`com.apple.security.files.bookmarks.collection-scope`
Read-only access to files the user has selected using an Open or Save dialog	`com.apple.security.files.user-selected.read-only`
Read-only access to files the user has selected using an Open or Save dialog	`com.apple.security.files.user-selected.read-only`
Read/write access to files the user has selected using an Open or Save dialog	`com.apple.security.files.user-selected.read-write`
Child process inheritance of the parent's sandbox	`com.apple.security.inherit`

Entitlements

Outgoing network socket for connecting to other machines	`com.apple.security.network.client`
Incoming network socket for listening for requests from other machines	`com.apple.security.network.server`
Read/write access to contacts in the user's address book; allows apps to infer the default address book if more than one is present on a system	`com.apple.security.personal-information.addressbook`
Use of the Core Location framework for determining the computer's geographical location	`com.apple.security.personal-information.location`
Printing	`com.apple.security.print`

Exception Entitlements

- Temporary grants by Apple for issues that haven't been permanently dealt with
- May be altered or completely disappear in subsequent revisions of the OS
- Ex: Sending Apple Events, Home and Absolute path relative access

XPC


Least Privilege Separation

- Functionality is split into smaller executable components on a process level
- Each component has its own entitlements
- Use of Interprocess Communication to establish connection between main app and XPC components

The Benefits

- Functionality is partitioned
- Attackers can only affect a subset of your application
- Code reuse between apps

Demos

Migrating Existing Apps

Migration Manifest

- A plist file embedded in your app
- Facilitates moving files from old locations to new sandboxed folder


SANDBOXING'S
DIRTY
LITTLE
SECRETS


Unexpected Errors

- Sandbox violations can cause errors in places that you have not expected them
- Check for (and handle) error values on methods that you call
- Not doing so can cause unexpected app failures

AppleScript

- Receive & Respond to Apple events
- Can send Apple events to a specific app using temporary entitlement

The Story of Shmat

```
void *shmat(int shmid, const void *shmaddr, int shmflg);
```



The Bottom Line

- 3rd party frameworks, libraries or plug-ins are susceptible points of failure
- Test your app thoroughly to find and eliminate sandbox violations

MACTECH CONFERENCE 2012

TEE-BOY

Yesterday

The Good Ole Days!

+

=

3-5 Day Wait

Today

Download in Seconds
or Minutes

Cloud

MACTECH CONFERENCE 2012

Tomorrow

- All Apps on the Mac will be Sandboxed
- All Apps will be on the Mac App Store
- Entitlements will be expanded

Summary

- App Sandboxing protects your apps
- Entitlements guide your app's behavior
- XPC mitigates security issues by partitioning behavior into small processes
- Testing is critical to surface issues raised by sandbox violations

More Information

- Apple's Developer Forums
- App Sandbox Design Guide
- Daemons and Services Programming Guide

Boisy G. Pitre
@boisypitre