# What's New in Kext Development Sign here please...

#### Session 707 Jerry Cottingham Software Engineer Core OS IO Team

These are confidential sessions—please refrain from streaming, blogging, or taking pictures

# In This Session

- Kext Development Overview
- Developer ID program
- Your attention please

• You are here because you develop a kext

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext
  - Kexts require wired memory

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext
  - Kexts require wired memory
  - Mistakes are often fatal

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext
  - Kexts require wired memory
  - Mistakes are often fatal
  - Debugging is harder

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext
  - Kexts require wired memory
  - Mistakes are often fatal
  - Debugging is harder
- OK, OK, if you must...

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext
  - Kexts require wired memory
  - Mistakes are often fatal
  - Debugging is harder
- OK, OK, if you must...
  - Kernel Extension Programming Topics on developer.apple.com

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext
  - Kexts require wired memory
  - Mistakes are often fatal
  - Debugging is harder
- OK, OK, if you must...
  - Kernel Extension Programming Topics on developer.apple.com
  - Kernel Programming Guide on developer.apple.com

p a kext to avoid writing a kext

Topics on developer.apple.com developer.apple.com

- You are here because you develop a kext
- You know the top three reasons to avoid writing a kext
  - Kexts require wired memory
  - Mistakes are often fatal
  - Debugging is harder
- OK, OK, if you must...
  - Kernel Extension Programming Topics on developer.apple.com
  - Kernel Programming Guide on developer.apple.com

With great power comes great responsibility

#### p a kext to avoid writing a kext

#### Topics on developer.apple.com developer.apple.com



• A kext is a bundle that extends the kernel



- A kext is a bundle that extends the kernel
  - Kext = Kernel Extension



- A kext is a bundle that extends the kernel
  - Kext = Kernel Extension
  - Only available for OS X, not iOS



- A kext is a bundle that extends the kernel
  - Kext = Kernel Extension
  - Only available for OS X, not iOS
- Structured like any CFBundle



- A kext is a bundle that extends the kernel
  - Kext = Kernel Extension
  - Only available for OS X, not iOS
- Structured like any CFBundle
  - Binary in MacOS folder



- A kext is a bundle that extends the kernel
  - Kext = Kernel Extension
  - Only available for OS X, not iOS
- Structured like any CFBundle
  - Binary in MacOS folder
  - Info.plist describes properties



- A kext is a bundle that extends the kernel
  - Kext = Kernel Extension
  - Only available for OS X, not iOS
- Structured like any CFBundle
  - Binary in MacOS folder
  - Info.plist describes properties
    - CFBundleldentifier



- A kext is a bundle that extends the kernel
  - Kext = Kernel Extension
  - Only available for OS X, not iOS
- Structured like any CFBundle
  - Binary in MacOS folder
  - Info.plist describes properties
    - CFBundleldentifier
    - CFBundleVersion

Name	Kind
AppleSamplePCI.kext	Folder
Contents	Folder
Info.plist	Property List
MacOS	Folder
AppleSamplePCI	Unix Executable File

#### Very important to update this!



Specific file/folder permissions

- Specific file/folder permissions
  - Kexts must be owned by "root," group "wheel"

- Specific file/folder permissions
  - Kexts must be owned by "root," group "wheel"
  - Must only be writable by "root"

- Specific file/folder permissions
  - Kexts must be owned by "root," group "wheel"
  - Must only be writable by "root"
  - Permissions are deep (all items in bundle)

- Specific file/folder permissions
  - Kexts must be owned by "root," group "wheel"
  - Must only be writable by "root"
  - Permissions are deep (all items in bundle)
  - Incorrect permissions = no load

- Specific file/folder permissions
  - Kexts must be owned by "root," group "wheel"
  - Must only be writable by "root"
  - Permissions are deep (all items in bundle)
  - Incorrect permissions = no load
- Use kextutil -tn to verify your kext



• OS X 10.9 code signing verification for kexts







• OS X 10.9 code signing verification for kexts OS X 10.9 all kext's signatures are verified





• OS X 10.9 code signing verification for kexts OS X 10.9 all kext's signatures are verified • OS X 10.9 unsigned or invalid signatures are not fatal (with one exception)





- OS X 10.9 code signing verification for kexts
  - OS X 10.9 all kext's signatures are verified
  - OS X 10.9 unsigned or invalid signatures are not fatal (with one exception)
  - OS X 10.9 Signed kexts will not load on releases prior to OS X 10.8



- OS X 10.9 code signing verification for kexts
  - OS X 10.9 all kext's signatures are verified
  - OS X 10.9 unsigned or invalid signatures are not fatal (with one exception)
  - OS X 10.9 Signed kexts will not load on releases prior to OS X 10.8 Valid code signatures will eventually be mandatory for all kexts



- OS X 10.9 code signing verification for kexts
  - OS X 10.9 all kext's signatures are verified
  - OS X 10.9 unsigned or invalid signatures are not fatal (with one exception)
- OS X 10.9 Signed kexts will not load on releases prior to OS X 10.8 Valid code signatures will eventually be mandatory for all kexts • Use kextutil -tn to verify your kext



**Be prepared!** 

#### Kext Development Overview Kext loading


Auto-load



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected
  - Searches in /System/Library/Extensions



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected
  - Searches in /System/Library/Extensions
- On-demand



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected
  - Searches in /System/Library/Extensions
- On-demand
  - Load by explicit path kextload ~/AppleSamplePCI.kext



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected
  - Searches in /System/Library/Extensions
- On-demand
  - Load by explicit path kextload ~/AppleSamplePCI.kext
  - Load by CFBundleldentifier



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected
  - Searches in /System/Library/Extensions
- On-demand
  - Load by explicit path kextload ~/AppleSamplePCI.kext
  - Load by CFBundleldentifier
    - Searches in /System/Library/Extensions



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected
  - Searches in /System/Library/Extensions
- On-demand
  - Load by explicit path kextload ~/AppleSamplePCI.kext
  - Load by CFBundleldentifier
    - Searches in /System/Library/Extensions
- Kernel cache build



- Auto-load
  - IOKit Kexts auto-load when matching hardware detected
  - Searches in /System/Library/Extensions
- On-demand
  - Load by explicit path kextload ~/AppleSamplePCI.kext
  - Load by CFBundleldentifier
    - Searches in /System/Library/Extensions
- Kernel cache build
  - Searches in /System/Library/Extensions





cache build





#### • OS X 10.9 auto-load, on-demand load by CFBundleldentifier, and kernel

cache build

Searches in /System/Library/Extensions and /Library/Extensions





#### • OS X 10.9 auto-load, on-demand load by CFBundleldentifier, and kernel

- OS X 10.9 auto-load, on-demand load by CFBundleldentifier, and kernel cache build
  - Searches in /System/Library/Extensions and /Library/Extensions Must code sign kexts in /Library/Extensions





Auto-load and auto-search

/System /Library /Extensions



Auto-load and auto-search

/System /Library /Extensions



/Library /Application Support

Auto-load and auto-search

/System /Library /Extensions

/System /Library /Filesystems /Library /Application Support

Auto-load and auto-search

/System /Library /Extensions

/System /Library /Filesystems /Library /Filesystems

/Library /Application Support

Auto-load and auto-search

/System /Library /Extensions

/System /Library /Filesystems /Library /Filesystems

/Library /Application Support

/Library /StartupItems

Auto-load and auto-search

/System /Library /Extensions

/System /Library /Filesystems

/Library /Filesystems

Inside app bundles



/Library /Application Support

/Library /Startupltems

/Applications

Auto-load and auto-search

/System /Library /Extensions

/System /Library /Filesystems

/Library /Filesystems

Inside app bundles



/System /Library /Extensions

/System /Library /Filesystems /Library /Filesystems

/Library /Application Support

/Library /StartupItems





Auto-load and auto-search

/System /Library /Extensions

/System /Library /Filesystems /Library /Filesystems



/Library /Application Support

/Library /StartupItems

/Applications



**NEW! Auto-load and auto-search** 

Auto-load and auto-search

/System /Library /Extensions

/System /Library /Filesystems /Library /Filesystems /Library

/Application

Support

/Library /StartupItems

Must be signed!

/Applications

/Library /Extensions

**NEW!** Auto-load and auto-search



Auto-load, kexts required for rooting, or auto-searching of kexts

Auto-load, kexts required for rooting, or auto-searching of kexts
OS X 10.9, /Library/Extensions MUST be signed

- Auto-load, kexts required for rooting, or auto-searching of kexts OS X 10.9, /Library/Extensions MUST be signed OS X 10.9, /System/Library/Extensions (for compatibility)

- Auto-load, kexts required for rooting, or auto-searching of kexts
  - OS X 10.9, /Library/Extensions MUST be signed
  - OS X 10.9, /System/Library/Extensions (for compatibility)
  - OS X 10.8 and earlier, install unsigned kext in /System/Library/Extensions

- Auto-load, kexts required for rooting, or auto-searching of kexts
  - OS X 10.9, /Library/Extensions MUST be signed
  - OS X 10.9, /System/Library/Extensions (for compatibility)
  - OS X 10.8 and earlier, install unsigned kext in /System/Library/Extensions
- All other kexts

- Auto-load, kexts required for rooting, or auto-searching of kexts
  - OS X 10.9, /Library/Extensions MUST be signed
  - OS X 10.9, /System/Library/Extensions (for compatibility)
  - OS X 10.8 and earlier, install unsigned kext in /System/Library/Extensions
- All other kexts
  - Signed kexts CAN go into /Library/Extensions

- Auto-load, kexts required for rooting, or auto-searching of kexts
  - OS X 10.9, /Library/Extensions MUST be signed
  - OS X 10.9, /System/Library/Extensions (for compatibility)
  - OS X 10.8 and earlier, install unsigned kext in /System/Library/Extensions
- All other kexts
  - Signed kexts CAN go into /Library/Extensions
  - Do not install anywhere in /System



- Auto-load, kexts required for rooting, or auto-searching of kexts
  - OS X 10.9, /Library/Extensions MUST be signed
  - OS X 10.9, /System/Library/Extensions (for compatibility)
  - OS X 10.8 and earlier, install unsigned kext in /System/Library/Extensions
- All other kexts
  - Signed kexts CAN go into /Library/Extensions
  - Do not install anywhere in /System
  - Other common locations still OK



- Auto-load, kexts required for rooting, or auto-searching of kexts
  - OS X 10.9, /Library/Extensions MUST be signed
  - OS X 10.9, /System/Library/Extensions (for compatibility)
  - OS X 10.8 and earlier, install unsigned kext in /System/Library/Extensions
- All other kexts
  - Signed kexts CAN go into /Library/Extensions
  - Do not install anywhere in /System
  - Other common locations still OK
- May need to install two kexts for compatibility with multiple releases



### Developer ID Program Sign here please...

#### Developer ID Program Sign here please...

• Part of Mac Development Program


- Part of Mac Development Program
- Allows distribution of applications outside of Mac App Store



- Part of Mac Development Program
- Allows distribution of applications outside of Mac App Store Special Developer ID certificate for signing applications



- Part of Mac Development Program
- Allows distribution of applications outside of Mac App Store
- Special Developer ID certificate for signing applications
- New with OS X 10.9, certificate for signing applications and kexts







Getting your Developer ID certificate







 Getting your Developer ID certificate 1. Go to https://developer.apple.com/resources/developer-id/





 Getting your Developer ID certificate 1. Go to https://developer.apple.com/resources/developer-id/





# 2. Click on link to request Developer ID certificate for signing kexts

 Getting your Developer ID certificate 1. Go to https://developer.apple.com/resources/developer-id/ 3. Fill out form





# 2. Click on link to request Developer ID certificate for signing kexts

- Getting your Developer ID certificate
  - 1. Go to https://developer.apple.com/resources/developer-id/
  - 2. Click on link to request Developer ID certificate for signing kexts
  - 3. Fill out form
  - 4. Once form is approved, go to request a Developer ID certificate in the "Certificates, Identifier, and Profiles" area of Member Center







Select the certificates you want to generate.



**Important:** Xcode is the preferred method for requesting and automatically installing these certificates on a Mac. Learn how



This certificate is used to code sign your app or kernel extension for distribution outside of the Mac App Store.

**Developer ID Installer** 

This certificate is used to sign your app's Installer Package for distribution outside of the Mac App Store.





- Part of Mac Development Program
- Allows distribution of applications outside of Mac App Store
- Special Developer ID certificate for signing applications
- New with OS X 10.9, certificate for signing applications, and kexts
- For more info

  - https://developer.apple.com/resources/developer-id/ See session 702 from WWDC 2012 (Gatekeeper and Developer ID)

signature verification error



#### Kexts in /Library/Extensions will not load if they are unsigned or have a

- signature verification error
- User will see the "no load" alert dialog



#### Kernel extension could not be loaded

The kernel extension at "/Library/Extensions/ AppleSamplePCI.kext" can't be loaded because it is from an unidentified developer. Extensions loaded from /Library/Extensions must be signed by identified developers.

Please contact the kernel extension vendor for updated software.





#### Kexts in /Library/Extensions will not load if they are unsigned or have a



a signature verification error



#### Kexts outside /Library/Extensions will load if they are unsigned or have

- a signature verification error
- But user will see the "unidentified developer" alert dialog



#### Kernel extension is not from an identified developer

The kernel extension at "/Users/local/ AppleSamplePCI.kext" is not from an identified developer but will still be loaded.

Please contact the kernel extension vendor for updated software.



#### • Kexts outside /Library/Extensions will load if they are unsigned or have



Code signature verification warnings and error messages



- Code signature verification warnings and error messages
- Most common code signature verification error codes



- Code signature verification warnings and error messages
- Most common code signature verification error codes
  - -67030 : something in kext bundle was modified



- Code signature verification warnings and error messages
- Most common code signature verification error codes
  - -67030 : something in kext bundle was modified
  - -67062 : kext is not code signed



- Code signature verification warnings and error messages Most common code signature verification error codes
- -67030 : something in kext bundle was modified
  - -67062 : kext is not code signed
  - Code signing error codes are in Security.framework: #include <Security/CSCommon.h>

- Code signature verification warnings and error messages Most common code signature verification error codes -67030 : something in kext bundle was modified
- - -67062 : kext is not code signed
  - Code signing error codes are in Security.framework:
    - #include <Security/CSCommon.h>

com.apple.kextd[40]: WARNING - Invalid signature -67030 for kext URL = "file:///Users/local/AppleSamplePCI.kext/", ID = "com.example.applesamplecode.driver.SamplePCI"

After modified Info.plist

Sign your kext with Developer ID certificate

- Sign your kext with Developer ID certificate
- Get out of /System/Library/Extensions
- certificate sions

- Sign your kext with Developer ID certificate
- Get out of /System/Library/Extensions
   In fact ALL of /System
   Talk to us in the set of the set

# certificate

#### Talk to us if you think you need to be here!

- Sign your kext with Developer ID certificate
- Get out of /System/Library/Extensions
  - In fact ALL of /System
- Get into /Library/Extensions

# certificate

#### Talk to us if you think you need to be here!

### What's New in Kext Development A sign of the times

#### Session 707 Dean Reece Core OS IO Team Manager

These are confidential sessions—please refrain from streaming, blogging, or taking pictures

### Building a Signed Kext for OS X 10.9 The tools

Use OS X 10.8.3 or later
Required for correct signing

### Building a Signed Kext for OS X 10.9 The tools

Use OS X 10.8.3 or later
Required for correct signing
Use Xcode 4.6 or later
Xcode 5.0 preferred

### Building a Signed Kext for OS X 10.9 The tools

- Use OS X 10.8.3 or later Required for correct signing
- Use Xcode 4.6 or later
  - Xcode 5.0 preferred
- - Acquire from Apple Developer website
  - Install in your keychain

# Requires Developer ID certificate for Applications and Kernel Extensions

### Building a Signed Kext for OS X 10.9 New Xcode project

No Loading			No	No Issues		
Choose a template for your new project						
<ul> <li>iOS</li> <li>Application</li> <li>Framework &amp; Library</li> <li>Other</li> <li>OS X</li> <li>Application</li> <li>Framework &amp; Library</li> <li>Application Plug-in</li> <li>Other</li> </ul>	Generic C++ Plug-in Ceneric C++ Plug-in Preference Pane	<image/> <section-header><section-header><image/><image/></section-header></section-header>	Image Unit Plug-in Creen Saver	<section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header>	tion	
	Generic K This template builds a	<b>Cernel Extension</b> kernel extension.			tercepts mouse- ends an action it object when - Intercepts ts and sends an a target	
Cancel Previous Next						
				Baundad T	and Bridden	

### Building a Signed Kext for OS X 10.9 New Xcode project

000	St 100	ding		No				
	Choose a template for your new project							
	<ul> <li>iOS</li> <li>Application Framework &amp; Library Other</li> <li>OS X</li> <li>Application Framework &amp; Library Application Plug-in</li> <li>Other</li> </ul>	Generic C++ Plug-in Freference Pane	<image/> <image/> <image/> <image/> <image/>	inage Unit Plug-in Creen Saver	<text></text>	tion		
72-	AND	Generic K This template builds a	<b>Cernel Extension</b> kernel extension.			tercepts mouse- ends an action it object when - Intercepts ts and sends an a target		
	Cancel Previous Next							
#### Building a Signed Kext for OS X 10.9 New Xcode project

Examplate for your new project iOS Application Framework & Library Other OS X Application Framework & Library Application Framework & Library Application Plug-in
Application Framework & Library Other OS X Application Framework & Library Application Plug-in
iOS Application Framework & Library Other OS X Application Framework & Library Application Plug-in
System Plug-in Other Preference Pane Qu <b>IOKit Driver</b> This template builds an IOK
7 IGM



#### Building a Signed Kext for OS X 10.9 New Xcode project

Examplate for your new project iOS Application Framework & Library Other OS X Application Framework & Library Application Framework & Library Application Plug-in
Application Framework & Library Other OS X Application Framework & Library Application Plug-in
iOS Application Framework & Library Other OS X Application Framework & Library Application Plug-in
System Plug-in Other Preference Pane Qu <b>IOKit Driver</b> This template builds an IOK
7 IGM



#### Building a Signed Kext for OS X 10.9 New Xcode project



	No Issu	es			
ur new project:					
				tior	1
leSamplePCI Company, Inc.					
.example					
.example.AppleSamplePCI					
				terce ends t obj	pts mouse- an action ect when
				- Int ts and a tar	ercepts d sends an get
	Previo	ous	Next	down n me	n – events ssage to
			Baumdad -	Fasternad D	

- Set SDK and Deployment for OS X 10.9
- Enable code signing
- Install kext in /Library/Extensions

#### In "Architectures" section

- Set Architecture to "Standard Architectures"
- Set Base SDK to Latest OS X (OS X 10.9)

				R M			
► ■   A> ■ My	AppleSamplePC	I: <b>Ready</b>   Today at	9:17 AM	No Issues			
🏭   🔺 🕨   📄 AppleSamp	lePCI						
			Build Settings	Build Phases	Build Rules		
PROJECT AppleSamplePCI	Basic A	I Combined	Levels		Q- Architectures		3
TARGETS	Architect	ures					
AppleSamplePCI	Setting			5	AppleSamplePCI		
AppleSamplePCIClient		Additional SDKs					
+ Add Target	Architectures			5	Standard Architectures (64-bit Intel) - \$(ARCHS_STANDARD) Latest OS X (OS X 10.9) <multiple values=""></multiple>		
		Base SDK					
	Build Active Architecture Only						
		Debug		1	res 🛊		
		Release		1	No \$		
Supported Platforms			orms	(	DS X \$		
		Valid Architectu	res	13	386 x86_64		
	▼ Linking						

#### chitectures" X 10.9)

#### In "Architectures" section

- Set Architecture to "Standard Architectures"
- Set Base SDK to Latest OS X (OS X 10.9)

00			Apple 🔁		R M		
▶	Mac 6	AppleSamplePC	I: <b>Ready</b>   Today at	No Issues			
🏭   🔺 🕨   🔄 AppleSamp	lePCI						
•			Build Settings	Build Phases	Build Rules		
PROJECT AppleSamplePCI	Basic A	II Combine	d Levels		Q- Architectures		3
TARGETS	Architect	ures					
AppleSamplePCI	Setting				C AppleSamplePCI		
AppleSamplePCIClient		Additional SDK	5				
+ Add Target		Architectures Base SDK Weild Active Architecture Only			Standard Architectures (64-bit Intel) - \$(ARCHS_STANDARD) Latest OS X (OS X 10.9) <multiple values=""></multiple>		
	,						
		Debug		Y	res 🛊		
		Release		N	No 🗘		
		Supported Platf	orms	C	os x 🛊		
		Valid Architectu	ires	13	886 x86_64		
	▼ Linking						

#### chitectures" X 10.9)

# In "Code Signing" section

Set "Code Signing Identity" to Developer ID: \*

		AppleS	SamplePCI.xcode	proj	N N
► ■   A> ■ My	Mac 6	ppleSamplePCI: <b>Ready</b>   Today at 9	9:17 AM	No Issues	
🏭   🔺 🕨   📄 AppleSamp	lePCI				
		Build Settings	Build Phases	Build Rules	
PROJECT AppleSamplePCI	Basic All	Combined Levels		Q- Code Signing	8
TARGETS AppleSamplePCI	Code Signin     S	<b>g</b> etting	Ç	AppleSamplePCI	
AppleSamplePCIClient	C	ode Signing Entitlements			
+ Add Target	C	ode Signing Resource Rules Path		eveloper ID: ***	
	0	ther Code Signing Flags			
	P	rovisioning Profile	N	lone 🗘	

# In "Code Signing" section

Set "Code Signing Identity" to Developer ID: \*

		Apples	SamplePCI.xcode	proj	N N
►	A> My Mac 6 AppleSamplePCI: Ready   Today at 9:17 AM			No Issues	
🏭   🔺 🕨   渣 AppleSampl	ePCI				
•		Build Settings	Build Phases	Build Rules	
PROJECT AppleSamplePCI	Basic A	I Combined Levels		Q- Code Signing	8
TARGETS AppleSamplePCI	Code Sign	ning Setting	¢	AppleSamplePCI	
AppleSamplePCIClient		Code Signing Entitlements			
+ Add Target		Code Signing Identity	C	Developer ID: * ‡	
		Code Signing Resource Rules Path			
		Other Code Signing Flags			
		Provisioning Profile	N	None 🗘	

#### In "Deployment" section

- Set Installation Directory to "/Library/Extensions"
- Set OS X Deployment Target to OS X 10.9

		AppleSamplePCI.xcodeproj					IN IN
► ■   A> ■ My	A > My Mac 6 AppleSamplePCI: Ready   Today at 9:17 AM			No Issues			
🏭   🔺 🕨   🙍 AppleSample	ePCI						
•		Build Settings	Build Phases	Build Rules			
PROJECT	Basic All	Combined Levels		Q- Deployment	l		8
AppleSamplePCI							
TARGETS	Deployment	t					
AppleSamplePCI	S	etting	Ċ	AppleSamplePCI			
AppleSamplePCIClient	Ir	nstall Group	w	heel			
+ Add Target	Ir	nstall Owner	ro	ot			
	Ir	nstall Permissions	a-	-w,u+w,a+rX			
	In	nstallation Build Products Location	/t	mp/AppleSamplePCI.dst			
	Ir	nstallation Directory	/L	ibrary/Extensions			
	0	S X Deployment Target	0	S X 10.9 🛟			
	P	re-install Requirements Property List					
	, SI	kip Install	N	0 🗘			

#### orary/Extensions" OS X 10.9

#### In "Deployment" section

- Set Installation Directory to "/Library/Extensions"
- Set OS X Deployment Target to OS X 10.9

		AppleSa			ľ	त्व १		
► ■   A> ■ My	A> My Mac 6 AppleSamplePCI: Ready   Today at 9:17 AM			No Issues				
🏭   🔺 🕨   🙍 AppleSampl	ePCI							_
٩		Build Settings	Build Phases	Build Rules				
PROJECT	Basic Al	Combined Levels		Q- Deployment			¢	3)
AppleSamplePCI								1
TARGETS	Deployme	ent						
AppleSamplePCI		Setting	C	AppleSamplePCI				
AppleSamplePCIClient		Install Group	w	heel				
+ Add Target		Install Owner	ro	oot				
		Install Permissions	a-	-w,u+w,a+rX				
		Installation Build Products Location	/t	mp/AppleSamplePCI.dst				
		Installation Directory	/L	ibrary/Extensions				
		OS X Deployment Target	0	S X 10.9 🛊				
		Pre-install Requirements Property List						
	,	Skip Install	N	lo 🗘				

#### orary/Extensions" OS X 10.9

• Kexts may only use Kernel.framework Applications may not use Kernel.framework

- Kexts may only use Kernel.framework
  - Applications may not use Kernel.framework
- OSObject (sub)classes must use OSDeclare\* and OSDefine\* macros
  - Required for release-to-release binary compatibility
  - Without, kext will not load on future releases
  - See OSMetaclass.h

- Kexts may only use Kernel.framework
  - Applications may not use Kernel.framework
- OSObject (sub)classes must use OSDeclare\* and OSDefine\* macros
  - Required for release-to-release binary compatibility
  - Without, kext will not load on future releases
  - See OSMetaclass.h
- Must not strip necessary symbols from kext binary
  - Safe to use strip -S -x

Builds one kext

- Builds one kext
- Kext should load on OS X 10.9 without warnings or alerts

- Builds one kext
- Kext should load on OS X 10.9 without warnings or alerts
- Use IIdb for kernel debugging Requires OS X 10.9 on both host and system under test

- Builds one kext
- Kext should load on OS X 10.9 without warnings or alerts
- Use IIdb for kernel debugging Requires OS X 10.9 on both host and system under test
- After packaging, verify installed into in /Library/Extensions

## Building a Kext for OS X 10.8 and Later Add a build target

- Start with OS X 10.9 kext example
- Add a 2nd kext target for OS X 10.8 kext
- Same values used for initial project setup

		🔄 Apple	SamplePCI.xcode	proj	IL IL
► ■   A> ■ My	My Mac 6 AppleSamplePCI: Ready   Today at 9:17 AM			No Issues	
🏭   🔺 🕨   🙍 AppleSample	ePCI				
٩		Build Settings	Build Phases	Build Rules	
PROJECT AppleSamplePCI	Basic All Con	bined Levels		Q- Deployment	8
TARGETS	Deployment				
🦈 AppleSamplePCI	Setting			AppleSamplePCI	
AppleSamplePCIClient	Install Gr	oup	W	heel	
+ Add Target	Install O	vner	r	oot	
	Install Pe	rmissions	a	-w,u+w,a+rX	
	Installatio	n Build Products Location	/1	tmp/AppleSamplePCI.dst	
	Installati	on Directory	1	Library/Extensions	
	OS X Dep	oyment Target	C	OS X 10.9 \$	
	Pre-instal	Requirements Property L	ist		
	, Skip Insta	1	٢	No 🗘	

## Building a Kext for OS X 10.8 and Later Add a build target

- Start with OS X 10.9 kext example
- Add a 2nd kext target for OS X 10.8 kext
- Same values used for initial project setup

AppleSample	ePCI.xcodeproj	II.	
. AppleSamplePCI: <b>Ready</b>   Today at 9:17 Al	M No Issues		
Build Settings Bui	ld Phases Build Rules		
All Combined Levels	Q- Deployment	8	
ployment			
Setting	C AppleSamplePCI		
Install Group	wheel		
Install Owner	root		
Install Permissions	a-w,u+w,a+rX		
Installation Build Products Location	/tmp/AppleSamplePCI.dst		
Installation Directory	/Library/Extensions		
OS X Deployment Target	OS X 10.9 \$		
Pre-install Requirements Property List			
Skip Install	No 🗘		
	AppleSamplePCI: Ready Today at 9:17 A Build Settings Bui AII Combined Levels  Oloyment Setting Install Group Install Owner Install Permissions Installation Build Products Location Installation Directory OS X Deployment Target Pre-install Requirements Property List Skip Install	AppleSamplePCI: Ready Today at 9:17 AM No Issues     Build Settings Build Phases Build Rules     Build Combined Levels Crepployment     Setting AppleSamplePCI   Install Group wheel   Install Owner root   Install Permissions a-w,u+w,a+rX   Installation Build Products Location /tmp/AppleSamplePCI.dst   Installation Directory /Library/Extensions   OS X Deployment Target OS X 10.9 \$   Pre-install Requirements Property List No \$	



			Apple:	SamplePCI.xco	deproj
A> 🛄 My	Mac 6	Indexing   2 f	iles remaining		No Iss
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic Al	Combine	d Levels		Q- Kernel N
	<b>Kernel Mo</b>	dule			
PCI		Setting			AppleSamplePCI
PCI_10.8		Module Identi	fier		com.example.apple-sam
PCIClient		Module Versio	2.2.0		
			Apple:	SamplePCI.xco	deproj
A) 🛄 My	Mac 6	Indexing   2 f	iles remaining		No Iss
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic Al	Combine	d Levels		Q- Kernel N
	▼ Kernel Mo	dule			
PCI		Setting			AppleSamplePCI_10.8
PCI_10.8		Module Identi	fier		com.example.apple-sam
PCIClient		Module Versio	'n		2.1.0



• Under "Kernel Module"



			Apple:	SamplePCI.xco	deproj
A> 🛄 My	Mac 6	Indexing   2 f	iles remaining		No Iss
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic Al	Combine	d Levels		Q- Kernel N
	<b>Kernel Mo</b>	dule			
PCI		Setting			AppleSamplePCI
PCI_10.8		Module Identi	fier		com.example.apple-sam
PCIClient		Module Versio	n		2.2.0
			Apple:	SamplePCI.xco	deproj
A) 🛄 My	Mac 6	Indexing   2 f	iles remaining		No Iss
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic Al	Combine	d Levels		Q- Kernel N
	▼ Kernel Mo	dule			
PCI		Setting			AppleSamplePCI_10.8
PCI_10.8		Module Identi	fier		com.example.apple-sam
PCIClient		Module Versio	'n		2.1.0



• Under "Kernel Module"

 "Module Identifier" must be same

0		)	
	>		
	◄	▶	
•			
PRO	JECT	Ē	
	App	leSar	nple
TAR	GET	S	
۲	Арр	leSar	nple
0	App	leSar	nple
	App	leSar	nple
(+)	Add	Targ	get
0			
~		-	
	>		1
	> <		
		•	
PRO		►	
PRO	JECT	► IeSar	nple
PRO TAR		► IeSar	nple
PRO PRO TAR	JECT App GET: App	leSar IeSar	nple
PRO PRO TAR	JECT App GET: App App	IeSar IeSar	nple nple
PRO PRO C	JECT App GET App App App	IeSar leSar leSar leSar	nple nple
PRO PRO C	JECT App GET: App App App Add	IeSar leSar leSar leSar Tarç	nple nple nple

	AppleSamplePCI.>	kcodeproj
A) 🛄 My	Mac 6 Indexing   2 files remaining	No Iss
AppleSamp	lePCI	
	Build Settings Build Pha	ses Build Rules
lePCI	Basic All Combined Levels	Q- Kernel N
	▼ Kernel Module	
lePCI	Setting	AppleSamplePCI
lePCI_10.8	Module Identifier	com.example.apple-sam
lePCIClient	Module Version	2.2.0
	AppleSamplePCI.	codeproj
A> 🛄 My	Mac 6 Indexing   2 files remaining	No Iss
AppleSamp	lePCI	
	Build Settings Build Pha	ses Build Rules
lePCI	Basic All Combined Levels	Q* Kernel N
	▼ Kernel Module	
lePCI	Setting	AppleSamplePCI_10.8
lePCI_10.8	Module Identifier	com.example.apple-sam
lePCIClient	Module Version	2.1.0



- Under "Kernel Module"
  - "Module Identifier" must be same
  - "Module Version" must be lower for OS X 10.8 target



			👌 Apple	SamplePCI.xco	deproj
A> 💻 My	Mac 6	Indexing   2 fi	les remaining		No Issi
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic All	Combined	Levels		Q- Kernel M
	▼ Kernel Mo	dule			
PCI		Setting			AppleSamplePCI
PCI_10.8		Module Identifi	ier		com.example.apple-sam
PCIClient		Module Versio	n		2.2.0
	-				
			Apple	SamplePCI.xco	deproj
A> 🛄 My	Mac 6	Indexing   2 fi	les remaining		No Issi
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic All	Combined	Levels		Q- Kernel M
	▼ Kernel Mo	dule			
PCI		Setting			AppleSamplePCI_10.8
PCI 10.8		Module Identifi	ier		com.example.apple-sam
PCIClient		Module Versio	n		2.1.0



- Under "Kernel Module"
  - "Module Identifier" must be same
  - "Module Version" must be lower for OS X 10.8 target
  - Necessary for OS to select correct kext

•	0 (	)	
]	>		l
	∢	▶	
•			
PRO	OJEC	Г	
	Арр	leSa	mp
TA	RGET	S	
	Арр	leSa	mp
ę	App	leSa	mp
	App	leSa	mp
+	Add	Targ	get.
-	0		_
0	00	)	
		,	1
		)     >	
		) 	
		)	mpl
		)	mpl
	OJECT App RGET	) I I I I I I I I I I I I I I I I I I I	mpl
	OJEC App App App	) I I I I I I I I I I I I I	mpl mpl
	OJEC App App App App	) I I I I I I I I I I I I I	mpl mpl mpl
	OJEC App App App App App Add	leSar	mpl mpl mpl get.

			Apple:	SamplePCI.xco	deproj
A> 🛄 My	Mac 6	Indexing   2 f	iles remaining		No Iss
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic Al	Combine	d Levels		Q- Kernel N
	<b>Kernel Mo</b>	dule			
PCI		Setting			AppleSamplePCI
PCI_10.8		Module Identi	fier		com.example.apple-sam
PCIClient		Module Versio	n		2.2.0
			Apple:	SamplePCI.xco	deproj
A) 🛄 My	Mac 6	Indexing   2 f	iles remaining		No Iss
AppleSamp	lePCI				
			Build Settings	Build Phases	Build Rules
PCI	Basic Al	Combine	d Levels		Q- Kernel N
	▼ Kernel Mo	dule			
PCI		Setting			AppleSamplePCI_10.8
PCI_10.8		Module Identi	fier		com.example.apple-sam
PCIClient		Module Versio	'n		2.1.0



- Set SDK and Deployment for OS X 10.8
- Disable code signing
- Install kext in /System/Library/Extensions

#### In "Architectures" section

- Set Architecture to "Standard Architectures"
- Set Base SDK to OS X 10.8

		AppleSamplePCI.xcodeproj	R
► ■   A> ■ My	Mac 6 Indexing   2 files remaining	No Issues	
🏭   🔺 🕨   📄 AppleSamp	lePCI		
٩	Build Settin	gs Build Phases Build Rules	
PROJECT AppleSamplePCI	Basic All Combined Levels	Q- Architectures	0
TARGETS AppleSamplePCI	Architectures Setting	AppleSamplePCI_10.8	
AppleSamplePCI_10.8	Additional SDKs		
AppleSamplePCIClient	Architectures	Standard Architectures (64-bit Intel) - \$(ARCHS_STANDARD) \$	
+ Add Target	Base SDK	OS X 10.8 ‡	
	Build Active Architecture Only	<multiple values=""> 🖨</multiple>	
	Debug	Yes ‡	
	Release	No 🗘	
	Supported Platforms	OS X ‡	
	Valid Architectures	i386 x86_64	
	▼ Linking		

#### In "Architectures" section

- Set Architecture to "Standard Architectures"
- Set Base SDK to OS X 10.8

		AppleSamplePCI.xcodeproj	ুল x
► ■   A> ■ My	Mac 6 Indexing   2 files remaining	g No Issues 📔 🗹 🗌 🗖 🔲	
🏭   🔺 🕨   📄 AppleSamp	lePCI		
٩	Build Set	tings Build Phases Build Rules	
PROJECT AppleSamplePCI	Basic All Combined Levels	Q- Architectures	8
TARGETS AppleSamplePCI	Architectures Setting	AppleSamplePCI_10.8	
AppleSamplePCI_10.8	Additional SDKs		
AppleSamplePCIClient	Architectures	Standard Architectures (64-bit Intel) - \$(ARCHS_STANDARD) \$	
+ Add Target	Base SDK	OS X 10.8 ‡	
And a second	Build Active Architecture O	nly <multiple values=""> \$</multiple>	
	Debug	Yes 🛊	
	Release	No 🗘	
	Supported Platforms	OS X \$	
	Valid Architectures	i386 x86_64	
	▼ Linking		

#### In "Code Signing" section

Set "Code Signing Identity" to "Don't Code Sign"

		AppleSamplePCI.xcodeproj	N N N N N N N N N N N N N N N N N N N
► ■   A> ■ My	Mac 6 Indexing   2 files remain	ning No Is	sues
🏭   🔺 🕨   📄 AppleSamp	ePCI		
•	Build S	ettings Build Phases Build Rules	
PROJECT AppleSamplePCI	Basic All Combined Leve	els Q* Code S	igning
TARGETS	▼ Code Signing		
AppleSamplePCI	Setting	AppleSamplePCI_10.8	3
AppleSamplePCI_10.8	Code Signing Entitlement	S	
AppleSamplePCIClient	Code Signing Identity	Don't Code Sign 🗘	
+ Add Target	Code Signing Resource R	ules Path	
	Other Code Signing Flags		
	Provisioning Profile	None 🗘	

#### In "Code Signing" section

Set "Code Signing Identity" to "Don't Code Sign"

00	👌 Apple	SamplePCI.xcodeproj	N N
▶	Mac 6 Indexing   2 files remaining	No Issues	
🏭   🔺 🕨   🔄 AppleSamp	lePCI		
٩	Build Settings	Build Phases Build Rules	
PROJECT AppleSamplePCI	Basic All Combined Levels	Q- Code Signing	8
TARGETS	▼ Code Signing		
AppleSamplePCI	Setting	AppleSamplePCI_10.8	
AppleSamplePCI_10.8	Code Signing Entitlements		
AppleSamplePCIClient	Code Signing Identity	Don't Code Sign \$	
+ Add Target	Code Signing Resource Rules Path		
	Other Code Signing Flags		
	Provisioning Profile	None 🗘	

#### In "Deployment" section

- Set Installation Directory to "/System/Library/Extensions"
- Set OS X Deployment Target to OS X 10.8

	AppleSample	PCI.xcodeproj	IN IN
▶	Mac 6 Indexing   2 files remaining	No Issues	
🏭   🔺 🕨   🚺 AppleSampl	ePCI		
•	Build Settings Build	l Phases Build Rules	
PROJECT AppleSamplePCI	Basic All Combined Levels	Q- Deployment	8
TARGETS	Deployment		
AppleSamplePCI	Setting	AppleSamplePCI_10.8	
AppleSamplePCI_10.8	Install Group	wheel	
AppleSamplePCIClient	Install Owner	root	
+ Add Target	Install Permissions	a-w,u+w,a+rX	
And a second	Installation Build Products Location	/tmp/AppleSamplePCI.dst	
	Installation Directory	/System/Library/Extensions	
	OS X Deployment Target	OS X 10.8 \$	
	Pre-install Requirements Property List		

#### stem/Library/Extensions" OS X 10.8

#### In "Deployment" section

- Set Installation Directory to "/System/Library/Extensions"
- Set OS X Deployment Target to OS X 10.8

	AppleSamp	lePCI.xcodeproj	IN IN
► ■   A> ■ My	Mac 6 Indexing   2 files remaining	No Issues	
🏭 🔺 🕨 📄 🔤 AppleSampl	lePCI		
•	Build Settings Bu	uild Phases Build Rules	
PROJECT AppleSamplePCI	Basic All Combined Levels	Q* Deployment	8
TARGETS	Deployment		
AppleSamplePCI	Setting	AppleSamplePCI_10.8	
AppleSamplePCI_10.8	Install Group	wheel	
AppleSamplePCIClient	Install Owner	root	
+ Add Target	Install Permissions	a-w,u+w,a+rX	
	Installation Build Products Location	/tmp/AppleSamplePCI.dst	
	Installation Directory	/System/Library/Extensions	
	OS X Deployment Target	OS X 10.8 ‡	
	Pre-install Requirements Property List		

#### stem/Library/Extensions" OS X 10.8

#### Building a Kext for OS X 10.8 and Later Build, test, and deploy

Builds two kexts

## Building a Kext for OS X 10.8 and Later Build, test, and deploy

- Builds two kexts
- Signed kext
  - Should load on OS X 10.9 without warnings or alerts
  - Use IIdb to debug
  - Verify installed into /Library/Extensions

## Building a Kext for OS X 10.8 and Later Build, test, and deploy

- Builds two kexts
- Signed kext
  - Should load on OS X 10.9 without warnings or alerts
  - Use IIdb to debug
  - Verify installed into /Library/Extensions
- Unsigned kext
  - Should load on OS X 10.8
  - Use gdb to debug
  - Verify installed into /System/Library/Extensions
- Builds two kexts
- Signed kext
  - Should load on OS X 10.9 without warnings or alerts
  - Use IIdb to debug
  - Verify installed into /Library/Extensions
- Unsigned kext
  - Should load on OS X 10.8
  - Use gdb to debug

 Verify installed into /System/Library/Extensions • Consider Installer script to avoid installing OS X 10.8 kext on OS X 10.9

### Building a Kext for OS X 10.7 and Later The tools

Use OS X 10.8.3 or later
Required for correct signing

### Building a Kext for OS X 10.7 and Later The tools

Use OS X 10.8.3 or later
Required for correct signing
Use Xcode 4.6—not Xcode 5.0
Required for OS X 10.7 SDK

### Building a Kext for OS X 10.7 and Later The tools

- Use OS X 10.8.3 or later Required for correct signing
- Use Xcode 4.6—not Xcode 5.0 Required for OS X 10.7 SDK
- - Acquire from Apple Developer website
  - Install in your keychain

Requires Developer ID certificate for Applications and Kernel Extensions

### Building a Kext for OS X 10.7 and Later Add a build target

 Same two-target approach as previously shown OS X 10.9 target identical

### Building a Kext for OS X 10.7 and Later Add a build target

- Same two-target approach as previously shown • OS X 10.9 target identical
- 2nd target has slightly different settings
  - OS X 10.7 SDK and deployment target
  - Need to add 32-bit architecture
  - Resulting kext will work on OS X 10.7 and OS X 10.8



			AppleSamplePCI.	xcodeproj	
<b>A</b> ⟩ My N	Mac 32-bit	Build Su	icceeded   Yesterd	ay at 5:20 PM	
AppleSample	ePCI				
			Build Settings	Build Phases	Build R
ePCI	Basic All Combine	ed Levels			Q- Kernel M
	Setting		AppleSamplePC		
ePCI	Module Identifier		com.example.app	le-samplecode.dr	iver.Sample
ePCI_10.7 ePCIClient	Module Version		2.2.0		p
A → My N	Mac 32-bit	Build Su	AppleSamplePCI.	xcodeproj ay at 5:20 PM	
AppleSample	ePCI				
			Build Settings	Build Phases	Build R
ePCI	Basic All Combine	ed Levels	AppleSampleP(	1 10 7	Q- Kernel N
	V Kernel Module		AppleSamplere	10.7	
ePCI	Module Identifier		com.example.app	le-samplecode.dr	iver.Sample
ePCI_10.7	Module Version		2.1.0		-
ePCIClient					

	(ball			
	9			
	_			
ules				
Module				
	-			
PCI				
_				
_				
	ð			
	_			
ules				
Aodule				
PCI				

• Under "Kernel Module"



			AppleSamplePCI.	xcodeproj	
<b>A</b> ⟩ My N	Mac 32-bit	Build Su	icceeded   Yesterd	ay at 5:20 PM	
AppleSample	ePCI				
			Build Settings	Build Phases	Build R
ePCI	Basic All Combine	ed Levels			Q- Kernel M
	Setting		AppleSamplePC		
ePCI	Module Identifier		com.example.app	le-samplecode.dr	iver.Sample
ePCI_10.7 ePCIClient	Module Version		2.2.0		p
A → My N	Mac 32-bit	Build Su	AppleSamplePCI.	xcodeproj ay at 5:20 PM	
AppleSample	ePCI				
			Build Settings	Build Phases	Build R
ePCI	Basic All Combine	ed Levels	AppleSampleP(	1 10 7	Q- Kernel N
	V Kernel Module		AppleSamplere	10.7	
ePCI	Module Identifier		com.example.app	le-samplecode.dr	iver.Sample
ePCI_10.7	Module Version		2.1.0		-
ePCIClient					

	(ball			
	9			
	_			
ules				
Module				
	-			
PCI				
_				
_				
	ð			
	_			
ules				
Aodule				
PCI				

• Under "Kernel Module"

 "Module Identifier" must be same



			AppleSamplePCI.x	codeproj	
<b>A</b> ⟩ My N	Mac 32-bit	Build S	ucceeded   Yesterda	y at 5:20 PM	
AppleSample	ePCI				
		1	Build Settings	Build Phases	Build R
ePCI	Basic All Combined	Levels			Q- Kernel M
	Setting		AppleSamplePCI		
-PCI	▼Kernel Module				
	Module Identifier		com.example.apple	e-samplecode.d	river.Sample
ePCI_10.7	Module Version		2.2.0		
ePCIClient					
			AppleSamplePCI.x	codeproi	
		Build S	ucceeded Vesterday	v at 5:20 PM	
<b>A</b> <i>⟩</i> My M	Mac 32-bit	bund 5	acceded   resterua	y at 5.20 m	
AppleSample	ePCI				
		1	Build Settings	Build Phases	Build R
ePCI	Basic All Combined	Levels			Q- Kernel M
	Setting		AppleSamplePCI	_10.7	
-PCI	▼Kernel Module				
	Module Identifier		com.example.apple	e-samplecode.d	river.Sample
ePCI_10.7	Module Version		2.1.0		
ePCIClient					

		X
	_	_
ules	5	
۸od	ule	
PCI		
_	_	_
-1		M
		ILC:AI
_	_	-
ules	5	
۸od	ule	
PCI		

- Under "Kernel Module"
  - "Module Identifier" must be same
  - "Module Version" must be lower for OS X 10.7 target



			AppleSamplePCI.>	codeproj	
A > My N	Mac 32-bit	Build Su	ucceeded   Yesterda	y at 5:20 PM	
AppleSample	PCI				
			Build Settings	Build Phases	Build R
ePCI	Basic All Combined	Levels			Q- Kernel M
	Setting		AppleSamplePC	l	
a PCI	▼Kernel Module				
arci	Module Identifier		com.example.appl	e-samplecode.d	river.Sample
ePCI_10.7	Module Version		2.2.0		
A > My N	Mac 32-bit	Build Su	AppleSamplePCI.>	xcodeproj y at 5:20 PM	
AppleSample	PCI				
		-	Build Settings	Build Phases	Build R
PCI	Basic All Combined	Levels			Q- Kernel M
	Setting		AppleSamplePC	_10.7	
ePCI	WKernel Module	_			
ePCI 10.7	Module Identifier		com.example.appl	e-samplecode.d	river.Sample
ePCIClient	Module Version		2.1.0		

ules	
Aodule	
_	
ules	
Aodule	
PCI	

- Under "Kernel Module"
  - "Module Identifier" must be same
  - "Module Version" must be lower for OS X 10.7 target
  - Necessary for OS to select correct kext



			AppleSamplePCI.	xcodeproj	
<b>A</b> ⟩ My N	Mac 32-bit	Build Su	icceeded   Yesterd	ay at 5:20 PM	
AppleSample	ePCI				
			Build Settings	Build Phases	Build R
ePCI	Basic All Combine	ed Levels			Q- Kernel M
	Setting		AppleSamplePC		
ePCI	Module Identifier		com.example.app	le-samplecode.dr	iver.Sample
ePCI_10.7 ePCIClient	Module Version		2.2.0		p
A → My N	Mac 32-bit	Build Su	AppleSamplePCI.	xcodeproj ay at 5:20 PM	
AppleSample	ePCI				
			Build Settings	Build Phases	Build R
ePCI	Basic All Combine	ed Levels	AppleSampleP(	1 10 7	Q- Kernel N
	V Kernel Module		AppleSamplere	10.7	
ePCI	Module Identifier		com.example.app	le-samplecode.dr	iver.Sample
ePCI_10.7	Module Version		2.1.0		-
ePCIClient					

	(ball			
	9			
	_			
ules				
Module				
	-			
PCI				
_				
_				
	ð			
	_			
ules				
Aodule				
PCI				

#### In "Architectures" section

- Set Architecture to "Standard (32/64-bit Intel)"
- Set Base SDK to OS X 10.7

		🔼 Apple		
► ( ■ A ) My	Mac 32-bit	Build Succeed		
🏭 🔺 🕨 🔀 AppleSamp	lePCI			
PROJECT		Build		
AppleSamplePCI	Basic All Combined I	evels		
TARCETS	Setting	1 🔿 A		
TARGETS	▼ Architectures			
ApplesamplerCl	Additional SDKs			
AppleSamplePCI_10.7	Architectures	Star		
AppleSamplePCIClient	Base SDK	OS		
	▼ Build Active Architecture Only	<mi< td=""></mi<>		
	Debug	Yes		
	Release	No		
	Supported Platforms	OS X		
	Valid Architectures			
	▼ Linking			
	Order File			
	▼Apple LLVM compiler 4.2 - Code C	Generation		

eSamplePCI.	xcodeproj	N N N N N N N N N N N N N N N N N N N
led   Yesterd	ay at 5:20 PM	
d Settings	Build Phases	Build Rules
	(	Architectures
AppleSampleP(	CI_10.7	
ndard (32/64	-bit Intel) - \$(ARC	CHS_STANDARD_32_64_BIT) \$
X 10.7 ‡		
ultiple values>	> 🛊	
\$		
\$		
x \$		
5 x86_64		

#### In "Architectures" section

- Set Architecture to "Standard (32/64-bit Intel)"
- Set Base SDK to OS X 10.7

		Apple			
► ( ■ A ) My	Mac 32-bit	Succeed			
🏭 🔺 🕨 🔀 AppleSamp	lePCI				
PROJECT		Build			
AppleSamplePCI	Basic All Combined Levels				
TARGETS	Setting	1© A			
	▼ Architectures				
AppleSampleRCL 10.7	Additional SDKs				
AppleSamplePCI_10.7	Architectures	Star			
AppleSamplePCIClient	Base SDK	OS			
	Build Active Architecture Only	<mı< td=""></mı<>			
	Debug	Yes			
	Release	No			
	Supported Platforms	OS >			
	Valid Architectures				
	▼ Linking				
	Order File				
	<b>WApple LLVM compiler 4.2 - Code Generation</b>				

eSamplePCI.	xcodeproj		N N
led   Yesterda	ay at 5:20 PM		
d Settings	Build Phases	Build Rules	
	(	<b>Q</b> Architectures	0
AppleSamplePC	CI_10.7		
ndard (32/64	-bit Intel) - \$(ARC	CHS_STANDARD_32_64_BIT) \$	
vitiple values>	. <u>*</u>		
\$			
x \$			
5 x86_64			

### In "Code Signing" section

Set "Code Signing Identity" to "Don't Code Sign"

			AppleSamplePCI.	xcodeproj		M <sub>21</sub>
► ( ■ ( A ) My (	Mac 32-bit	Build S	ucceeded   Yesterd	ay at 5:20 PM		
🔛 🔍 🕨 🔁 AppleSampl	ePCI					
PROJECT			Build Settings	Build Phases	Build Rules	
AppleSamplePCI	Basic All Comb	ned Levels			Q- Code Signing	(3)
TARGETS AppleSamplePCI AppleSamplePCI_10.7 AppleSamplePCIClient	Setting ▼Code Signing Code Signing Entitleme Code Signing Identity Code Signing Resource	nts Rules Path	Don't Code Sign	CI_10.7		
	Other Code Signing Flag	IS				

### In "Code Signing" section

Set "Code Signing Identity" to "Don't Code Sign"

Build Succeeded Yesterday at 5:20 PM     PROJECT     AppleSamplePCI     Basic     Combined   Levels     Setting     Code Signing     Code Signing Identity        Code Signing Resource Rules Path        Other Code Signing Flags				AppleSamplePC	.xcodeproj		R <sub>M</sub>
PROJECT   AppleSamplePCI   TARGETS   AppleSamplePCI   AppleSamplePCI   AppleSamplePCI   Code Signing   Code Signing Identity   Don't Code Sign \$   Code Signing Resource Rules Path   Other Code Signing Flags	► ( ■ A ) My I	Mac 32-bit	Build S	ucceeded   Yesterd	lay at 5:20 PM		
PROJECT   AppleSamplePCI   TARGETS   AppleSamplePCI   AppleSamplePCI   Code Signing Entitlements   Code Signing Identity   Don't Code Sign \$   Code Signing Resource Rules Path   Other Code Signing Flags	🏭 🔺 🕨 🔁 AppleSampl	ePCI					
AppleSamplePCI   Basic All Combined Levels   Code Signing   Setting   AppleSamplePCI   Code Signing Intilements   Code Signing Identity   Code Signing Resource Rules Path   Other Code Signing Flags	PROJECT			Build Settings	Build Phases	Build Rules	
Setting       AppleSamplePCI_10.7         AppleSamplePCI_10.7       Code Signing Entitlements         Code Signing Identity       Don't Code Sign \$         Code Signing Resource Rules Path       Other Code Signing Flags	AppleSamplePCI	Basic All Con	bined Levels			Q- Code Signing	3
	TARGETS   AppleSamplePCI_10.7   AppleSamplePCIClient	Setting Code Signing Entitler Code Signing Identity Code Signing Resour Other Code Signing F	nents , ce Rules Path lags	Oon't Code Sign	CI_10.7		

#### In "Deployment" section

- Set Installation Directory to "/System/Library/Extensions"
- Set OS X Deployment Target to OS X 10.7

		Apple			
► ( ■ A ) My	Mac 32-bit	ucceed			
🏭 🔺 🕨 🔀 AppleSamp	lePCI				
PROJECT		Build			
AppleSamplePCI	Basic All Combined Levels				
TARGETS	Setting	1© A			
AppleSamplePCI	<b>V</b> Deployment				
	Install Group	whee			
AppleSamplePCI_10.7	Install Owner	root			
AppleSamplePCIClient	Install Permissions				
	Installation Build Products Location				
	Installation Directory				
	OS X Deployment Target				
	Pre-install Requirements Property List				
	Skip Install	No			
	Install Group	whe			
	Install Owner	root			
	Install Permissions	a-w,			

#### stem/Library/Extensions" OS X 10.7

eSamplePCI.xcodep	oroj	N N N N N N N N N N N N N N N N N N N
led   Yesterday at 5:2	0 PM	
d Settings Build	Phases	Build Rules
	Q	Deployment
AppleSamplePCI_10.7		
el ,u+w,a+rX p/AppleSamplePCI.dst stem/Library/Extension X 10.7 \$ el t	ons	
,u+w,a+rX		

#### In "Deployment" section

- Set Installation Directory to "/System/Library/Extensions"
- Set OS X Deployment Target to OS X 10.7

		Apple		
► ( ■ A ) My	Mac 32-bit	ucceed		
🏭 🔺 🕨 🔀 AppleSampl	lePCI			
PROJECT		Build		
AppleSamplePCI	Basic All Combined Levels			
TARGETS	Setting	10 A		
AppleSamplePCI	▼ Deployment			
	Install Group Install Owner Install Permissions			
AppleSamplePCI_10.7				
AppleSamplePCIClient				
	Installation Build Products Location			
	Installation Directory	/Sys		
	OS X Deployment Target			
	Pre-install Requirements Property List			
	Skip Install	No		
	Install Group	whe		
	Install Owner	root		
	Install Permissions	a-w		

#### stem/Library/Extensions" OS X 10.7

eSamplePCI.x	codeproj	N N N N N N N N N N N N N N N N N N N
l <b>ed</b> ∣ Yesterda	y at 5:20 PM	
d Settings	Build Phases	Build Rules
		Q- Deployment
AppleSamplePCI	_10.7	
el		
:		
,u+w,a+rX		
p/AppleSample	PCI.dst	
stem/Library/E	Extensions	
X 10.7 🛟		
\$		
el		
:		
,u+w,a+rX		

Builds two kexts

- Builds two kexts
- Signed kext
  - Should load on OS X 10.9 without warnings or alerts
  - Use IIdb to debug
  - Verify installed into /Library/Extensions

- Builds two kexts
- Signed kext
  - Should load on OS X 10.9 without warnings or alerts
  - Use IIdb to debug
  - Verify installed into /Library/Extensions
- Unsigned kext
  - Should load on OS X 10.7 and OS X 10.8
  - Use gdb to debug
  - Verify installed into /System/Library/Extensions

- Builds two kexts
- Signed kext
  - Should load on OS X 10.9 without warnings or alerts
  - Use IIdb to debug
  - Verify installed into /Library/Extensions
- Unsigned kext
  - Should load on OS X 10.7 and OS X 10.8
  - Use gdb to debug

 Verify installed into /System/Library/Extensions • Consider Installer script to avoid installing OS X 10.8 kext on OS X 10.9

- If you need to target releases prior to OS X 10.7
  - Create two or more kext projects
  - Must use prior versions of Xcode for older SDKs
  - May need to build on multiple OS releases

- If you need to target releases prior to OS X 10.7
  - Create two or more kext projects
  - Must use prior versions of Xcode for older SDKs
  - May need to build on multiple OS releases
- OS X 10.9 kext project installs in /Library/Extensions

- If you need to target releases prior to OS X 10.7
  - Create two or more kext projects
  - Must use prior versions of Xcode for older SDKs
  - May need to build on multiple OS releases
- OS X 10.9 kext project installs in /Library/Extensions
- Target other OS releases with additional project(s)
  - Follow compatibility guidance from those releases
  - Install unsigned kext(s) in /System/Library/Extensions

- If you need to target releases prior to OS X 10.7
  - Create two or more kext projects
  - Must use prior versions of Xcode for older SDKs
  - May need to build on multiple OS releases
- OS X 10.9 kext project installs in /Library/Extensions
- Target other OS releases with additional project(s)
  - Follow compatibility guidance from those releases
  - Install unsigned kext(s) in /System/Library/Extensions
- Installer script can skip kexts for releases older than target OS volume

# **Compatibility Summary**

	To Support	OS X 10.7+	OS X 10.8+	OS X 10.9
	Development System	OS X 10.8.3+		
		Xcode 4.6	Xcode 4.6 or 5.0	
OS X 10.9 Target	SDK and Deployment	OS X 10.9		
	Code Sign	Developer ID		
	Install Path	/Library/Extensions		
Legacy Target	SDK and Deployment	OS X 10.7	OS X 10.8	n/a
	Code Sign	Don't Code Sign		n/a
	Install Path	/System/Library/Extensio	n/a	



# IIdb Kernel Debugging Or, how I learned to love debugging and ignore the bomb

#### Session 707 Brian Bechtel Core OS Panic Triage

These are confidential sessions—please refrain from streaming, blogging, or taking pictures

# Your first 10,000 panics are the hardest to debug. After that, it gets somewhat easier.

# IIdb—A New, Powerful Debugger

- Integration with llvm and the rest of the development tool chain More knowledge shared between compiler and debugger
- Much faster
- Better supported and actively being developed





# IIdb—A New, Powerful Debugger

Extremely powerful Python scripting language
Lets you do anything Python can do
gdb to IIdb command map <a href="http://lldb.llvm.org/lldb-gdb.html">http://lldb.llvm.org/lldb-gdb.html</a>
The debugger for OS X 10.9 and beyond



# gdb is Dead

- gdb is gone in Xcode 5.0
  - No gdb binaries
  - No kgmacros file in Kernel Debug Kit for OS X 10.9 or later
  - No plan to fix any issues remaining
- Still the debugger of choice for OS X 10.8 and earlier
  - Available as part of Xcode 4.6



#### ig Kit for OS X 10.9 or later ing IS X 10 8 and earlier



### Demo zprint in gdb versus zprint in lldb

	Terminal	Shell	Edit	View	Window	Help	
00	0					0	DB — gdb-
(gdb)	zprint						
			I				
SVD	O					66	@amelio.a;
(lldb	) zprint[]						

db-i386-apple-d — 197×24

### 0.00

H M

10

apple.com -- IIdb -- 197×24

### 0.00
#### Standard kgmacros Are Still There Minor improvements in output format

paniclog backtrace showcurrentstacks showalltasks showallstacks zombproc zombstacks zprint showallkmods showallvmstats memstats systemlog showbootargs

### Adding Kext Symbols

- On startup IIdb will scan kexts installed in
  - /System/Library/Extensions
  - Library/Extensions
  - /Volumes/KernelDebugKit
  - Additional locations can be specified in ~/.lldbinit

settings set platform.plugin.darwin-kernel.kext-directories /tmp /a /b

Add additional kext symbols using the addkext macro



### Watch Out For

- "backtick" expression for evaluation x/i `myRoutine+0x18`
- Idb is pedantic about "->" versus "." p myStruct->myField
- May need to cast a variable very explicitly to display correctly p \*(struct myStruct\*)myVariable
- File bugs
  - http://bugreporter.apple.com

disassemble -f -m The entire current frame

disassemble -l -m The current line

disassemble -s {address} -e {address} -m From start address to end address In IIdb minimum abbreviations are allowed



(lldb) di -n fseventsf\_write -m mach\_kernel`fseventsf\_write at vfs\_fsevents.c:1537 unused int flags, \_\_unused vfs\_context\_t ctx) 1536 1537 { 1538 return EIO; 0xffffff800ae04810: pushq %rbp movq %rsp, %rbp 0xffffff800ae04811: 0xffffff800ae04814: movl \$5, %eax mach\_kernel`fseventsf\_write + 9 at vfs\_fsevents.c:1538 1537 { 1538 return EIO; 1539 ł 0xffffff800ae04819: %rbp popq 0xffffff800ae0481a: ret

(lldb) di -n fseventsf\_write -m mach\_kernel`fseventsf\_write at vfs\_fsevents.c:1537 <u>unused int flags</u>, <u>unused vfs\_context\_t ctx</u>) 1536 1537 { return EIO; 1538 0xffffff800ae04810: %rbp pushq 0xffffff800ae04811: %rsp, %rbp movq 0xffffff800ae04814: movl \$5, %eax mach\_kernel`fseventsf\_write + 9 at vfs\_fsevents.c:1538 1537 { 1538 return EIO; 1539 } 0xffffff800ae04819: %rbp popq 0xffffff800ae0481a: ret

(lldb) di -n fseventsf\_write -m mach\_kernel`fseventsf\_write at vfs\_fsevents.c:1537 <u>unused int flags</u>, <u>unused vfs\_context\_t ctx</u>) 1536 1537 { 1538 return EIO; 0xffffff800ae04810: %rbp pushq movq %rsp, %rbp 0xffffff800ae04811: 0xfffff800ae04814: movl \$5, %eax mach\_kernel`fseventsf\_write + 9 at vfs\_fsevents.c:1538 1537 { 1538 return EIO; 1539 ł 0xffffff800ae04819: %rbp popq 0xffffff800ae0481a: ret

(lldb) di -n fseventsf\_write -m mach\_kernel`fseventsf\_write at vfs\_fsevents.c:1537 \_\_\_unused int flags, \_\_unused vfs\_context\_t ctx) 1536 1537 { 1538 return EIO; 0xffffff800ae04810: pushq %rbp movq %rsp, %rbp 0xffffff800ae04811: 0xffffff800ae04814: movl \$5, %eax mach\_kernel`fseventsf\_write + 9 at vfs\_fsevents.c:1538 1537 { 1538 return EIO; 1539  $\mathbf{F}$ 0xffffff800ae04819: %rbp popq 0xffffff800ae0481a: ret

(lldb) di -n fseventsf\_write -m mach\_kernel`fseventsf\_write at vfs\_fsevents.c:1537 unused int flags, \_\_unused vfs\_context\_t ctx) 1536 1537 { 1538 return EIO; 0xffffff800ae04810: pushq %rbp movq %rsp, %rbp 0xffffff800ae04811: 0xffffff800ae04814: movl \$5, %eax mach\_kernel`fseventsf\_write + 9 at vfs\_fsevents.c:1538 1537 { 1538 return EIO; 1539 ł 0xffffff800ae04819: %rbp popq 0xffffff800ae0481a: ret

#### IIdb kgmacros Additional Arguments

- -o /tmp/foo
- -s search\_string
- -V
- -V -V -V

- # output to file /tmp/foo

  - # sets verbosity +1
  - # increases verbosity +3
- Example, to find load information for just "AppleSamplePCI.kext" showallkmods -s AppleSamplePCI

# grep for search\_string in output

#### Ildbmacros Precautions

- Ildbmacros do not automatically load in Ildb
  - prevents you from debugging a malicious application and getting evil Ildb macros from a hidden symbol file
- To overcome this, add to your ~/.lldbinit file
   settings set target.load-script-from-symbol-file true
- Add custom python to Resources/Python in your kext bundle AppleSamplePCI.kext.dSYM/Contents/Resources/Python/

#### Faster Loading, No Symbols

- To speed startup and not load all kext symbols, use settings set plugin.dynamic-loader.darwin-kernel.load-kexts false
- To load your kext symbols after connecting, the commands are addkext <uuid> : Load one kext based on uuid addkext -N <name> : Load one kext that matches the name provided addkext -F <abs/path/to/executable> <address> addkext all : Will load all the kext symbols - SLOW

#### Use nvram to Enable Debugging

- With no debug boot-args set, system automatically reboots on panic • OS X 10.8 or later
- Set boot-args using the nvram command line tool as root
  - Must reboot to let settings take effect
- debug flags are a bit map of behaviors
  - See table 20-1 of "Kernel Programming Guide"
  - E.g. 0x4 is DB NMI (drop into debugger on NMI)

#### Ways to Connect

- Built-in Ethernet
- Built-in Firewire (e.g. iMac)
- Thunderbolt->Ethernet adapter
- Thunderbolt-> Firewire adapter
- Apple Thunderbolt Display -> Ethernet
- Apple Thunderbolt Display -> Firewire
- No wireless, no USB

nernet ewire

#### kdp\_match\_name

- Two machine debugging assumes "network" port of en0 • If not, add "kdp\_match\_name={something}" to boot-args
- - {something} depends upon your connection
- if config will tell you appropriate ports

- Use ifconfig to find appropriate port name
- en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
  options=2b<RXCSUM,TXCSUM,VLAN\_HWTAGGING,TS04>
  ether 3c:07:54:27:8d:0b
  inet6 fe80::3e07:54ff:fe27:8d0b%en1 prefixlen 64 scopeid 0x4
  inet6 2620:149:4:202:3e07:54ff:fe27:8d0b prefixlen 64 autoconf
  inet6 2620:149:4:202:68ca:1665:6165:9944 prefixlen 64 autoconf temporary
  inet 10.0.40.2 netmask 0xffffc00 broadcast 10.0.255.255
  media: autoselect (1000baseT <full-duplex,flow-control>)
  status: active

Built-in Ethernet

sudo nvram boot-args="debug=0x144"

- Thunderbolt -> Ethernet
   sudo nvram boot-args="debug=0x144 kdp\_match\_name=en2"
- Apple Thunderbolt Display -> Ethernet
  sudo nvram boot-args="debug=0x144 kdp\_match\_name=en4"
  Use port from ifconfig instead of en4 or en2

- Native Firewire
  - sudo nvram boot-args="debug=0x144 kdp\_match\_name=firewire"
- Thunderbolt -> Firewire
   sudo nvram boot-args="debug=0x144 kdp\_match\_name=firewire fwkdp=0x8000"
- Apple Thunderbolt Display -> Firewire sudo nvram boot-args="debug=0x144 kdp\_mat
- sudo nvram boot-args="debug=0x144 kdp\_match\_name=firewire fwkdp=0x8000"
  Always reboot to let settings take effect

### Firewire Debugging

- In one terminal window
   fwkdp
- In a second terminal window

xcrun lldb /Volumes/KernelDebugKit/mach\_kernel
kdp-remote localhost

#### Connecting

xcrun lldb /Volumes/KernelDebugKit/mach\_kernel

- Avoid confusion; use xcrun
- Live

kdp-remote {name or ip} kdp-remote 10.0.1.25 kdp-remote mycomputer.local kdp-remote mycomputer.mydomain.com

Coredump

file --core {/path/to/file} file -c /PanicDumps/core-xnu-2050.22.13-10.0.1.25-47b8de62

## Just invoking IIdb might grab some horrible out of date monstrosity

#### Miscellaneous Notes

- We've changed NMI
- Coredumps how-to
- Zone corruption boot-args
- Console output and graphics

### We've Changed NMI in OS X 10.9

- With boot-args set so that debug has the 0x4 bit set, e.g.
   sudo nvram boot-args="debug=0x144"
- In OS X 10.8 or earlier, NMI was Power key alone
- Now it is Left-# + Right-# + Power
- You can revert to the old behavior by or'ing in the 0x8000 bit sudo nvram boot-args="debug=0x8144"

#### Automatically Save Coredumps

• Host (e.g. 10.0.40.2)

sudo mkdir /PanicDumps sudo chown root:wheel /PanicDumps sudo chmod 1777 /PanicDumps sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.kdumpd.plist

• Client (panicking machine)

sudo nvram boot-args="debug=0xd44 \_panicd\_ip=10.0.40.2" sudo reboot

#### **Zone Protection and Corruption Checks**

- Buffer overruns, use-after-free errors, zone-mismatched frees, and timing induced races
  - -ZC
  - zalloc code checks the free list pointers of all zones for correctness -zp
    - Catches attempts to execute or access freed data
  - zfree routine overwrites freed memory with 0xdeadbeefdeadbeef sudo nvram boot-args="debug=0x144 -zp -zc"

#### **Guard Mode Kernel Zone Allocator**

- gzalloc\_size=<size>
  - Target all zones with elements of <size> bytes
- gzalloc\_min=<size> gzalloc\_max=<size> Target zones with elements >= size or <= size</li>
- -gzalloc\_wp
  - Write protect, rather than unmap, freed allocations
  - -gzalloc\_wp requires gzalloc\_size or gzalloc\_min/max

#### Performance Considerations

- -zp and -zc add additional runtime checks
  - Little additional memory usage
- -gzalloc\_wp gzalloc\_size={size} takes much more memory Each allocation is a 4k page with additional guard page Measurably slower, but catches more bugs

### **Console Output and Graphics**

- Graphics changed to support multiple buffers • OS X 10.8 and later
- Draw to a buffer instead of directly to the screen Enhancement for retina display machines • Unreliable console output to the screen if you panic

#### More Information

Paul Danbold Core OS Evangelist danbold@apple.com

#### Documentation

Understanding and debugging kernel panics http://developer.apple.com/library/mac/#technotes/tn2063/\_index.html Kernel Core Dumps http://developer.apple.com/library/mac/#technotes/tn2004/tn2118.html Generating a Non-Maskable Interrupt (NMI) http://developer.apple.com/library/mac/#qa/qa1264/\_index.html WWDC 2012 Session 415:"Debugging with Ildb"

Apple Developer Forums http://devforums.apple.com

#### **Related Sessions**

Advanced Debugging with LLDB

Pacific Heights Friday 9:00AM



OS X Kernel Lab

OS X Kernel Lab

Core OS Lab B Wednesday 2:00PM	
Core OS Lab B Friday 10:15AM	

#### Summary

- Sign your kext in OS X 10.9
- IIdb is faster and more powerful
  Still have the kgmacros you know and love
- New ways of two machine debugging via Thunderbolt adapters
- New boot-args to track down bugs

ow and love gging via Thunderbolt adapters gs



# <u>É WWDC2013</u>