© Developer News Design Account **Developer Forums** Q Search by keywords or tags

Develop

Distribute

Q

Support

Resolving App Sandbox Inheritance Problems

Discover



This thread has been locked by a moderator.



This post is part of a cluster of posts related to the trusted execution system. If you found your way here directly, I recommend that you start at the top.

Share and Enjoy

© 292

Quinn "The Eskimo!" @ Developer Technical Support @ Apple let myEmail = "eskimo" + "1" + "@" + "apple.com"

Resolving App Sandbox Inheritance Problems

If you're creating a product with the App Sandbox enabled and it crashes with a trap within _libsecinit_appsandbox, it's likely that you're tripping over one of the following problems:

- Nonheritable entitlements
- Changing sandbox
- Nothing to inherit

Nonheritable Entitlements

The most common cause of this problem is also the most obscure. If you have a sandboxed app with an embedded program that you run as a child process, a crash in _libsecinit_appsandbox is most likely caused by the embedded program being signed with entitlements that can't be inherited.

Imagine an, SandboxInit, with an embedded helper tool, NotHeritable. When the app runs the helper tool as a child process, the helper tool crashes with a crash report like this:

```
Exception Type:
                        EXC_BAD_INSTRUCTION (SIGILL)
Thread O Crashed:: Dispatch queue: com.apple.main-thread
0 libsystem_secinit.dylib ... _libsecinit_appsandbox.cold.7 + 49
1 libsystem_secinit_dylib ... _libsecinit_appsandbox + 2096
2 libsystem_trace.dylib ... _os_activity_initiate_impl + 51
3 libsystem_secinit.dylib ... _libsecinit_initializer + 67
4 libSystem.B.dylib
                            ... libSystem_initializer + 286
5 dyld
                            ... invocation function for block in dyld4::Loade...
6 dyld
                            ... invocation function for block in dyld3::Mach0...
7 dyld
                            ... invocation function for block in dyld3::Mach0...
                            ... dyld3::MachOFile::forEachLoadCommand(Diagnost...
8 dyld
9 dyld
                            ... dyld3::MachOFile::forEachSection(void (dyld3:...
                            ... dyld3::MachOAnalyzer::forEachInitializer(Diag...
10 dyld
11 dyld
                            ... dyld4::Loader::findAndRunAllInitializers(dyld...
                            ... dyld4::APIs::runAllInitializersForMain() + 38
12 dyld
13 dyld
                            ... dyld4::prepare(dyld4::APIs&, dyld3::MachOAnal...
                            ... start + 388
14 dyld
```

The helper tool has trapped within _libsecinit_appsandbox. Look at the entitlements of the helper tool:

```
% codesign -d --entitlements - SandboxInit.app/Contents/MacOS/NotHeritable
[Dict]
    [Key] com.apple.security.app-sandbox
    [Value]
        [Bool] true
    [Key] com.apple.security.inherit
    [Value]
        [Bool] true
    [Key] com.apple.security.get-task-allow
    [Value]
        [Bool] true
```

The com.apple.security.app-sandbox and com.apple.security.inherit entitlements are fine: They configure the program to inherit its sandbox from its parent. The problem is the com.apple.security.get-task-allow entitlement, which is not compatible with this sandbox inheritance.

The com.apple.security.get-task-allow entitlement is often automatically injected by Xcode. For information on how to prevent this, see Embedding a Command-Line Tool in a Sandboxed App.

Some entitlements are compatible with sandbox inheritance. Unfortunately that list of entitlements is not documented (r. 93582428). The most commonly use ones are the hardened runtime exception entitlements documented in Hardened Runtime. The other entitlements on the list are pretty obscure.

Changing Sandbox

Another cause of a trap within _libsecinit_appsandbox is the child process trying to set up its own sandbox. If a sandboxed process runs another program as a child process, that child process always inherits its sandbox from the parent. If the program's executable is signed with com.apple.security.app-sandbox but not com.apple.security.inherit — that is, it tries to set up a new sandbox — it will crash in libsecinit appsandbox. A process is not allowed to change its sandbox.

To check for this problem, look for the following in the crash report:

```
Application Specific Signatures:
SYSCALL_SET_PROFILE
```

This indicates that the process tried to setup its sandbox profile but that failed, in this case because it already has a sandbox profile.

To fix this problem, either:

- In the child, add the com.apple.security.inherit entitlement so that it inherits its sandbox from the parent.
- In the parent, run the program so that it's not a child process. For example, you could launch it using NSWorkspace.

Nothing to Inherit

Another cause of a trap within _libsecinit_appsandbox is when a nonsandboxed process runs another program as a child process and that other program's executable has the com.apple.security.app-sandbox and com.apple.security.inherit entitlements. That is, the child process wants to inherit its sandbox from its parent but there's nothing to inherit.

To check for this problem, look for the following in the crash report:

```
Application Specific Information:
 Process is not in an inherited sandbox.
There are three ways you might fix this problem:
```

- Sandbox the parent.
- Unsandbox the child.
- Run the child in its own sandbox by removing the com.apple.security.inherit entitlement.

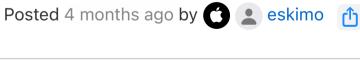
Gatekeeper Code Signing Notarization

Developer > Forums

To view the latest developer news, visit



Add a Comment



of any third parties in connection with or related to your use of the site. All postings and use of the content on this site are subject to the Apple Developer Forums Participation Agreement.

This site contains user submitted content, comments and opinions and is for informational purposes only. Apple disclaims any and all liability for the acts, omissions and conduct

Platforms	Topics & Technologies	Resources	Programs
iOS	Accessibility	Documentation	Apple Developer Program
iPadOS	Accessories	Curriculum	Apple Developer Enterprise Program
macOS	App Extensions	Downloads	App Store Small Business Program
tvOS	App Store	Forums	MFi Program
watchOS	Audio & Video	Videos	News Partner Program
Tools	Augmented Reality	Support Support Articles Contact Us	Video Partner Program
	Business		Security Bounty Program Security Research Device Program
Swift	Design		
SwiftUI	Distribution		
SF Symbols	Education	Bug Reporting	Events
Swift Playgrounds	Fonts	System Status	App Accelerators
TestFlight	Games	Account	App Store Awards
Xcode Cloud	Health & Fitness	Apple Developer App Store Connect Certificates, IDs, & Profiles	Apple Design Awards Apple Developer Academies Entrepreneur Camp
	In-App Purchase		
	Localization		
	Maps & Location	Feedback Assistant	Tech Talks
	Machine Learning	1 CCADACK ASSISTANT	WWDC
	Security		
	Safari & Web		

News and Updates