INFORMATION SECURITY

Dynamic analysis of Swift application using Cycript or gdb

Asked 4 years, 2 months ago Active 3 years, 11 months ago Viewed 2k times

3

I am doing analysis of a Swift iOS application. I am able to attach gdb or Cycript, but after that these tools are not able to do any method swizzling. I cant even call some method directly using Cycript, which is very easy in Objective C apps.

In gdb, I can set the breakpoint on the methods, but it's not able to detect the same method during execution. If there is a way for runtime analysis of Swift apps, please let me know.

3

mobile ios runtime

Share Improve this question

Follow

edited Dec 21 '16 at 18:10

Rory Alsop ♦

61.1k 11 112 310

asked Dec 21 '16 at 16:20

Saurabh

133 4

1 Answer

Active Oldest Votes

2

Michael Gianarakis spoke about reversing Swift including hooking at the Hack-in-the Box conference in 2016 -- http://gsec.hitb.org/materials/sg2016/COMMSEC%20D1%20-%20Michael%20Gianarakis%20-%20Reverse%20Engineering%20Swift%20Applications.pdf

In particular, Michael goes over function hooking on getter methods (which work) and setters (which do not), as also discussed here -- https://web.archive.org/web/20151004101419/http://www.eswick.com/2014/06/inside-swift/

Some additional notes on function hooking and the ability to work it all together with MSHookFunction from Substrate is available here -- https://www.securify.nl/blog/SFY20150302/hooking_swift_methods_for_fun_and_profit.html

Here also is an older article on Swift method swizzling -- https://www.uraimo.com/2015/10/23/effective-method-swizzling-with-swift/

Finally, Michael makes mention to using macOS tools such as `nm` and `xcrun` to engineer a Swift-aware `class-dump`, but you can also check out this one here -- https://github.com/BlueCocoa/class-dump/

Share Improve this answer Follow

answered Feb 13 '17 at 22:44

atdre
18.6k 5 56 105