iOS 9 Reverse Engineering with JavaScript

Frida (http://www.frida.re/) 6.0, released this week, includes brand new support for iOS 9. Whether you're doing security research on apps or system services, or you're an app developer wanting to trace API calls, this new release has got you covered.

As some of you may know, Frida can inject V8 into any process, on both desktop and mobile. This JavaScript runtime that Frida injects is conceptually just a language binding for Frida's instrumentation engine, frida-gum (https://github.com/frida/frida-gum). Beside letting you enumerate threads, loaded modules, hook arbitrary functions, call native APIs, etc., all implemented in C and assembly, there are also the ObjC and Java modules written in pure JavaScript. These leverage the aforementioned low-level primitives to give you easy access to the higher-level internals of any app or system service.

Now with Pangu's iOS 9 jailbreak and Apple's Kernel Patch Protection, it looks like we'll have to live without some of the kernel adjustments that were common in earlier jailbreaks. Among them was the patch lifting Apple's ban on RWX (Read-Write-Execute) memory pages, and this happens to be an important feature that the V8 engine was designed to take advantage of.

This was a challenge for Frida, depending on V8 for its JS runtime, but also a long-standing issue preventing us from instrumenting apps on non-jailbroken devices, where one could otherwise just repackage the app with Frida included and instrument away.

I am super-excited to announce that after weeks of coding here at NowSecure, with countless cups of coffee consumed, we are no longer dependent on V8. Yes, with Frida 6.0 we have a brand new JavaScript runtime based on JavaScriptCore. This is a system framework, so we don't even have to add that to our binary footprint. We do however still use V8 on other OSes, and kernels that support RWX pages, but it is no longer our achilles heel. Plus, Frida will soon be seen instrumenting apps on non-jailbroken devices.

So, that's iOS. What else is new? Something that kept coming up when building tools on top of Frida is that it would be very useful to collect details about the system you're instrumenting. Perhaps what kind of OS, architecture, IP addresses of network interfaces, etc. Exactly what kind of details are necessary really depends on the needs of your tool, and it doesn't really make sense to add all possible system information to Frida's APIs. There would always be something missing, and for everybody else there would be a lot of unnecessary complexity. Now with Frida 6.0 we have finally solved this. All you have to do is attach to pid 0, and you get a so-called system session running inside Frida itself. Scripts that you create here can inspect `Process.platform`, `Process.arch`, etc., or use `NativeFunction` to call an OS API, like say, for enumerating network interfaces (https://www.npmjs.com/package/frida-get-ifaddrs).

Beside these features, improved injection capabilities on OS X El Capitan, REPL improvements and many bug-fixes, this release also improves Frida's function hooking. That part is however a story of its own, but here's the TLDR for the technically curious: We added support for relocating more position-dependent instructions, and even take great care to allow you to hook functions that happen to reside in the libc. The challenge there is that with iOS 9, and other systems that don't permit RWX pages, for Frida to modify a function in order to hook it, it has to flip the memory page that it's on to RW (read-write), perform the modification, then flip it back to RX (read-execute). If, however, the function to be modified happens to fall on the same page as the libc function we use to change the page protection, then we obviously can't call it, as it's not currently executable. The solution is to perform that system-call ourselves (https://github.com/frida/frida-gum/commit/dedff3782b8b8cb9e58a92f5d99cbbe6dea62920).

I hope you enjoy this new release, and if you do please help spread the word! :) If for some reason Frida doesn't work for you, please do get in touch.

Posted by Ole André Vadla Ravnås (/blog/author/oleavr/) in Research (/blog/research/), Development (/blog/development/), Mobile Security (/blog/mobile-security/)
Monday, November 16th 2015
Tags: Frida (/blog/tag/frida/), Tools (/blog/tag/tools/), Open Source (/blog/tag/open-source/)

0 Comments NowSecure Blogs Исследовательс...

Recommend Share Sort by Newest

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Privacy DISQUS

CATEGORIES

Customer Success (/blog/customer-success/)	3
Development (/blog/development/)	57
Featured (/blog/featured/)	5
Forensics (/blog/forensics/)	372
Life at NowSecure (/blog/life-at-nowsecure/)	26
Mobile Security (/blog/mobile-security/)	723
News (/blog/news/)	132
Research (/blog/research/)	22
Threat Intelligence (/blog/threat-intelligence/)	2

TAGS

android (423) (/blog/tag/android/) android-m (1) (/blog/tag/android-m/) byod (25) (/blog/tag/byod/) blackberry (35) (/blog/tag/blackberry/)
blackphone (4) (/blog/tag/blackphone/) cve (2) (/blog/tag/cve/) google-io (1) (/blog/tag/google-io/) osx (1) (/blog/tag/osx/) r&d (1) (/blog/tag/r&d/) rsac (9) (/blog/tag/rsac/)
sdlc (6) (/blog/tag/sdlc/) windows (27) (/blog/tag/windows/) android (7) (/blog/tag/android/) appsecure (9) (/blog/tag/appsecure/)
application-development (22) (/blog/tag/application-development/) application-security (235) (/blog/tag/application-security/) applications (5) (/blog/tag/applications/)
arbitrary-code-execution (1) (/blog/tag/arbitrary-code-execution/) banking (55) (/blog/tag/banking/) biometrics (1) (/blog/tag/biometrics/) careers (23) (/blog/tag/careers/)
compliance (4) (/blog/tag/compliance/) data-insecurity (2) (/blog/tag/data-insecurity/) data-security (426) (/blog/tag/data-security/) definitions (49) (/blog/tag/definitions/)
detection (2) (/blog/tag/detection/) development (2) (/blog/tag/development/) device-security (169) (/blog/tag/device-security/) embedded (1) (/blog/tag/embedded/)
exploit (1) (/blog/tag/exploit/) finance (35) (/blog/tag/finance/) forensics (2) (/blog/tag/forensics/) frida (2) (/blog/tag/frida/) fuzzing (1) (/blog/tag/fuzzing/)
google (1) (/blog/tag/google/) government (72) (/blog/tag/government/) healthcare (2) (/blog/tag/healthcare/) howto (108) (/blog/tag/howto/) ios (178) (/blog/tag/ios/)
infographics (1) (/blog/tag/infographics/) intel (1) (/blog/tag/intel/) ios (4) (/blog/tag/ios/) malware (58) (/blog/tag/malware/) mobile-security (1) (/blog/tag/mobile-security/)
open-source (2) (/blog/tag/open-source/) oss (1) (/blog/tag/oss/) presentations (118) (/blog/tag/presentations/) press-releases (28) (/blog/tag/press-releases/)
privilege-escalation (1) (/blog/tag/privilege-escalation/) product-updates (92) (/blog/tag/product-updates/) real-estate (1) (/blog/tag/real-estate/)
research (2) (/blog/tag/research/) responsible-disclosure (2) (/blog/tag/responsible-disclosure/) security (2) (/blog/tag/security/) tools (249) (/blog/tag/tools/)
touchid (1) (/blog/tag/touchid/) training (23) (/blog/tag/training/) videos (26) (/blog/tag/videos/) vulnerabilities (169) (/blog/tag/vulnerabilities/)
vulnerability (2) (/blog/tag/vulnerability/) wearables (1) (/blog/tag/wearables/)

We are NowSecure™ (/)

NowSecure is advancing mobile security worldwide with nearly 300 million devices and app downloads protected by our technology

(https://twitter.com/nowsecuremobile)
(https://facebook.com/nowsecure)
(https://plus.google.com/b/117661237231493188465/117661237231493188465/)
(https://linkedin.com/company/nowsecure)

Products

Mobile App (https://www.nowsecure.com/#the-mobile-app)
App Testing (https://www.nowsecure.com/apptesting/)
BYOD (https://www.nowsecure.com/byod/)
Forensics (https://www.nowsecure.com/forensics/)

Company

About (https://www.nowsecure.com/company/)
Careers (https://www.nowsecure.com/careers/)
Services (https://www.nowsecure.com/services/)
Security Feed (https://www.nowsecure.com/security-feed/)

Resources

Blog (https://www.nowsecure.com/blog/)
Contact (https://www.nowsecure.com/contact/)
Press (https://www.nowsecure.com/press/)
Privacy & Security (https://www.nowsecure.com/privacy-security/)