Faster Mobile App Pentesting with Corellium

How a pentesting team at an Australian telecom saved time and money

An Australian telecommunications company serves a large consumer base and has a massive network. Their security pentesting team has a diverse range of technologies to test on a regular basis, from their own cloud-based application network, to web applications, to mobile applications for both Android and iOS. Testing iOS was particularly challenging until they adopted Corellium.

The challenge

A member of their pentesting team stated that the way they used to pentest iOS apps was a “cat and mouse game of balancing devices and apps.” They continually support the latest iPhone device models, with each device model supported for approximately two years. For example, as of 2022, devices ranging from iPhone 12 to iPhone 14 Pro are supported. With several iOS version updates per year, the resulting matrix testing suite is quite large and complex.

Since they were testing on physical devices, they needed to ship devices around the country to as many as 15 to 20 security pentesters at any given time.

iOS devices often needed to be jailbroken for adequate security testing and analytics. Typically, the team had to wait six months to a year for a publicly available iOS jailbreak to become available. And applying these jailbreaks to each device is not a small or quick task. It amounted to a lot of mundane work that cut into the time the team had to actually conduct mobile app pentests.

And as with all physical device and lab approaches, the continual procurement, configuration, bricking, and reimaging of devices is costly, tedious, and time consuming. There must be a better way.

The Solution

The company first learned of Corellium through a major accounting firm's recommendation. They needed to address using physical phones, accelerate their pentesting cycles, and test mobile apps more effectively.

The team at first used Corellium to test Android devices. After a while, the team started using Corellium for iOS as well, and found it to provide a much better security testing experience when compared to testing on physical devices. The telecommunications company found that no one else in the market offered the iOS testing features and functionality that Corellium provided.

"The biggest thing for us was the simplicity of being able to do something virtually that didn't involve us buying a heap of mobile devices, and all that sort of stuff."

With Corellium, the security testing team can spin-up a wide variety of virtual iPhone device models and iOS versions in a few clicks, both with and without jailbreaking. Full-stack testing of the OS, apps, data, and network layers is facilitated by a wide range of advanced security testing tools built into the Corellium platform. And one-click device snapshot, restore, and clone functionality greatly simplified their workflows and cross-team collaboration needs.

The Results

The learning curve for iOS testing with Corellium took a couple of months to reach its full potential, but it was well worth the effort. The team successfully uses Corellium for their iOS mobile app penetration testing needs.

"The biggest impact is that it increases the throughput and our ability to not be constrained by (physical) devices anymore."

Switching to Corellium led to measurable productivity gains. The team were able to do a lot more testing within a shorter time span, and they efficiently worked through their pentesting backlog.

Free trials at **Corellium.com**

CORELLIUM