CORELLIUM®

CASE STUDY

Large Telco Now Pentests 3x Faster

A leading U.S. telecommunications provider conquered their mobile security testing challenges with the help of Corellium.

The challenge

Security testing iOS apps can get pretty complicated. Apple releases multiple new iPhone devices each year. 2021 saw the release of the iPhone 13, iPhone 13 Mini, iPhone 13 Pro, and iPhone 13 Pro Max. 2022 has seen a similarly crowded iPhone 14 line and a third generation iPhone SE-- it's a lot to keep up with. And the iOS operating system also has updates a few times per year, so the combinations of iPhone models and iOS versions is ever compounding.

That complexity meant that the customer's security testing team had at least 20-25 devices at any given time to test on. If a mistake is made, it can brick the device, so a new one must be procured. That happened to the team at least a few times. Bricked devices upset team members as watching expensive devices become useless is frustrating.

These testing devices also had to be shipped between teams in three US states. It was a logistical challenge, delayed work, and could even introduce risks of being lost or stolen. As Apple continually increases the security of its products, the challenges of security testing and mobile app penetration testing teams also increases. Teams are often faced with not being able to install their own SSL certificates, jailbreak devices, or bypass locks on iOS bootloaders. Testing apps on the most recent iOS versions was difficult if not impossible, particularly as public jailbreaks are not available.

"Setting up a device could take a couple of weeks of work! It's tedious and boring and it's a complete waste of time for my team" according to the team leader.

The team had given iOS emulator solutions a try, but in the end they still had to do testing directly on physical phones. iOS emulation is notorious for how difficult and unreliable it can be, and it's not simple to replace SSL certificates in an emulator either.

The Solution

There had to be a better way. In their search for alternatives, the team discovered Corellium.

With the Corellium Virtual Hardware platform, the customer can easily spin-up near limitless combinations of virtual iPhone device models and iOS versions, jailbroken or not, with the click of a button. A wide range of advanced security testing tools are built into the platform for full-stack testing: OS, file, app, and network.

The ability to snapshot and clone virtual phones makes remote collaboration a snap for security testing between geographically separated teams. In a survey, an engineer on the team said using Corellium is “way easier” than the frustrating methodology they were stuck with previously. Finally, the security testing team could focus on their actual testing work without having to worry about cumbersome setup work and shipping times.

Before adopting Corellium, the team conducted multiple trials, and when the lead pentester (with ten years of mobile testing experience) gave Corellium a try, they were sold.

The Results

The team lead said they were able to conduct three times as many pentests in the time it used to take to conduct one pentest. Their use cases include mobile vulnerability research, static, dynamic, and network pentesting, reverse engineering, security training, and malware analysis. They used to only be able to test 30 of their iOS apps, but now they can test a lot more as they have approximately 150 customer-facing mobile apps. As for support from Corellium, **the team said in a survey that Corellium’s support and documentation “far exceeded our expectations.”**

Free trials at **Corellium.com**

CORELLIUM ®