GOVTECH SINGAPORE

iOS Reverse Engineering

GovTech Brownbag

Back Dynamic Analysis > Side-loading Modified Application

Side-loading Modified Application

By Max Chee

Explore how it is possible to side-load a modified application binary from the AppStore.

DIFFICULTY

ESTIMATED TIME

10 Minutes

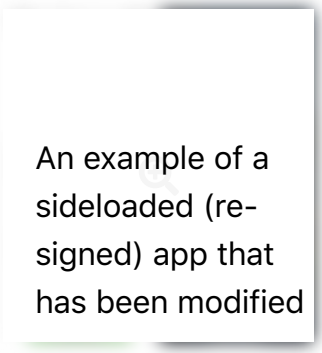
Exercise Summary

- Install apps outside of Apple app store
- Side loading is possible in iOS devices

Background

In this example, we will be showing how re-signed applications can be sideloaded into the phone. This technique allows an anyone to modify an original application's binary and sideload it onto any device. One of the main reason for sideloading is because in iOS security, installation of non-official apps is a critical step for security research. The aim of this exercise is to allow you to be less dependent on automated tools like Cydia Impactor/ReProvision. We will be using the following material in this exercise:

- frida-ios-dump
- Xcode
- iOS-deploy



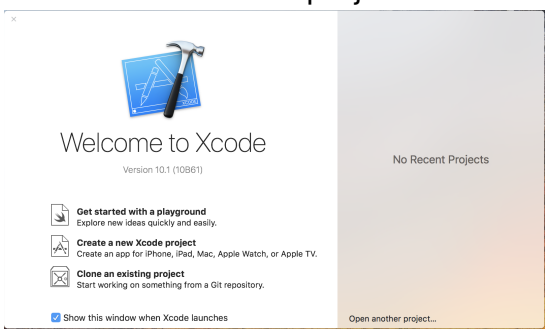
An example of a sideloaded (re-signed) app that has been modified

Sideloading Exercise

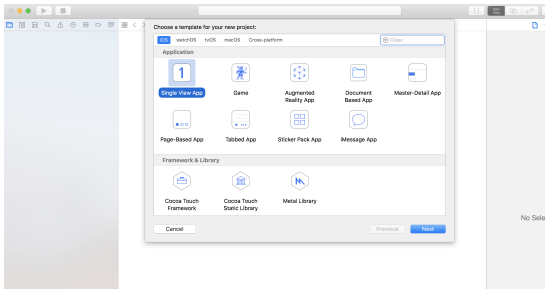
In this exercise, we will be referencing an application named Helix, this detailed step-by-step instruction guide is by courtesy of our friendly colleague from GovTech Eileen Tay.

Setting Up & Deploying Blank App

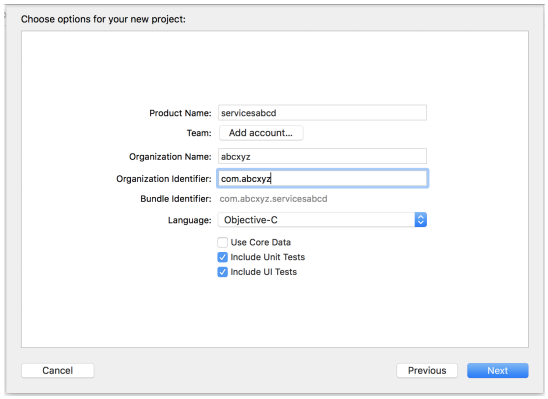
1. Create an empty base app with a free apple developer account.
    1. Create a new Xcode project



    2. Select Single View App for iOS



    3. Add dummy names like the following



    4. Add Developer account