GOVTECH SINGAPORE

iOS Reverse Engineering

GovTech Brownbag

Back Dynamic Analysis > Runtime Data Storage & Keychain

Runtime Data Storage & Keychain

By Max Chee

Developers may leave sensitive information in data storage/keychain during runtime under the false impression that a malicious entity will not be able to retrieve information from them. Explore how it is possible to retrieve information from keychain during runtime.

DIFFICULTY

ESTIMATED TIME

5 Minutes

Exercise Summary

- Inspect data storage on a jailbroken device
- Extract sensitive information from:
  - Keychain
  - Cookies
  - User Defaults

Background

In this example, we are showing an application that stores sensitive data in different locations. Developers may assume that storing sensitive data such as API secrets in keychains or other locations will be safe as user would not be able to access such data. We will explore how to retrieve these data using a tool called PassionFruit.

Different data storage and its uses

Keychain - Used to store chunks of data such as certificates and passwords
Cookies – Used to store session cookies
UserDefaults – Used to store key-value pairs persistently in app

Location for various data storage

Keychain
/private/var/Keychains
/keychain-2.db

Cookies
/private/var/mobile/**<App directory>**/Library/Cookies/
Cookies.binarycookies

UserDefaults
/private/var/mobile/**<App directory>**/Library
/Preferences/**<App Bundle>**.plist