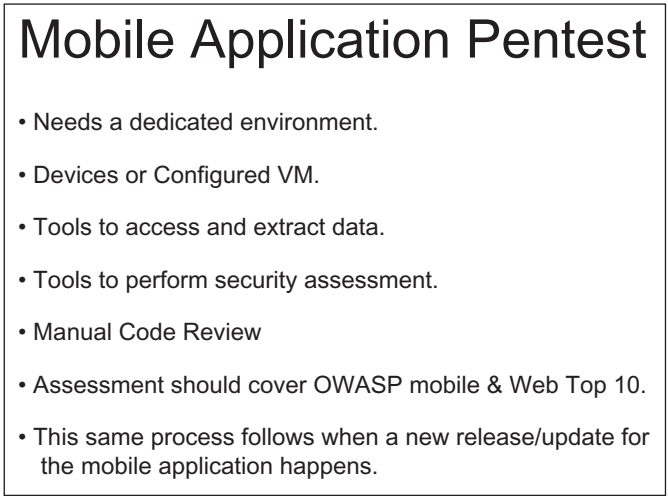
# CHAPTER 1

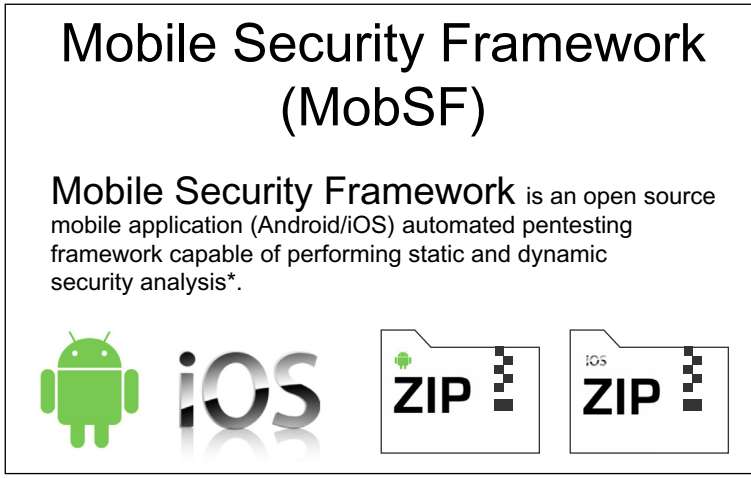
# The Mobile Application Pentest




Consider a typical mobile application pentest. You need to set up a dedicated environment. You should either have devices or configured virtual machines, like Android or iOS virtual machines or emulators. Then you need the right tools to access and extract the data in transit like HTTP(S) proxies, SQLite viewer for viewing SQLite DB files, and all those things etc. Again you need another set of tools for performing security assessment of mobile applications and another important aspect of mobile application pentest is a Manual Code Review. So you have to do the Manual Code Review; if it is an Android binary you have to decompile it, extract the source code, then do a code review on the source code. Or if it's a white box testing where you have access to the source code, you have to go to the source code and perform a security code review. Again the assessment should cover OWASP mobile top 10 and the OWASP Web Top 10 in case of hybrid application. So these days, mobile applications are mostly hybrid, they have both the mobile component as well as the web component in them. So the vulnerabilities that affect the mobile phase as well as the vulnerabilities that affect the web space are applicable in this context.

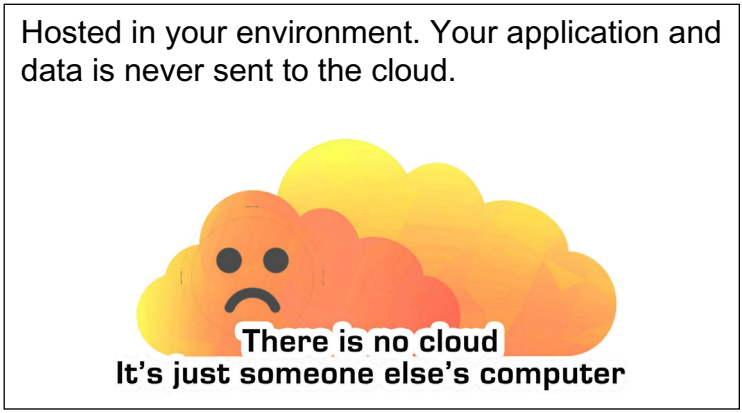
**Automated Security Analysis of Android and iOS Applications with Mobile Security Framework.**
**DOI:** http://dx.doi.org/10.1016/B978-0-12-804718-7.00001-1
© 2016 Elsevier Inc. All rights reserved.

Again the same process follows when a new release or update for the mobile application happens. This is really a cumbersome process. Whenever there is an update or a new major version release or change, you have to go through the whole process. And again it's not really an easy job. You have to have the entire environment ready and set up so that you can start testing a new application or a version update. So this really is a hectic process to setup and maintain the testing environment. And in this space comes the importance of mobile security framework.



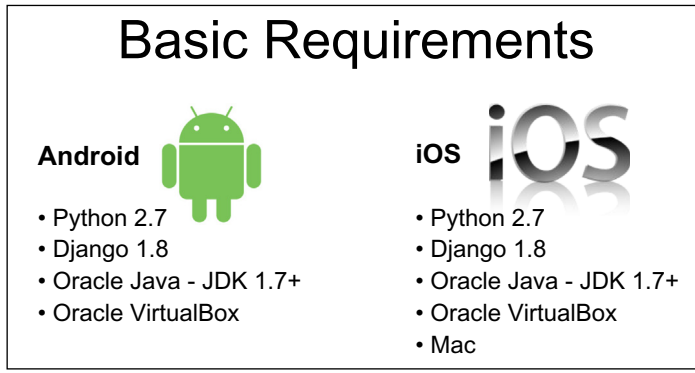

So Mobile Security Framework is an open source mobile application—Android/iOS automated pentesting framework capable of performing static and dynamic security analysis. The current version supports Android, compressed source code zip file, iOS compressed source code zip file; so any can be the input. As of now the framework only supports dynamic analysis of Android binaries. You can download it from github: https://github.com/ajinabraham/Mobile-Security-Framework-MobSF/, which is the project page of mobile security framework. The framework is multiplatform compatible; so as of now it runs in Windows, Linux, and Mac. When it comes to Linux, the tested and supported Linux operating system is Ubuntu.

When it comes to security assessment, there are a lot of security tools or products out there that works from the cloud.

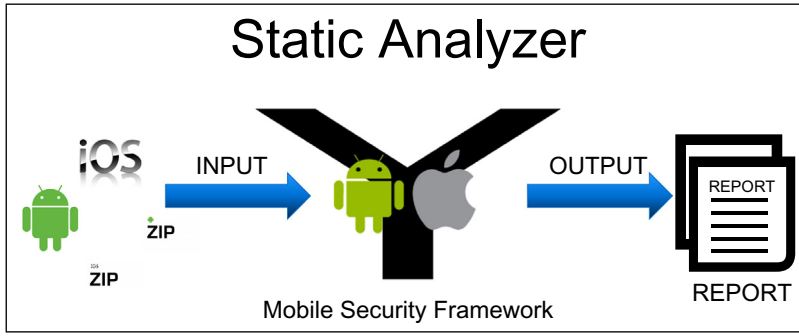



So there is the image that you don't have to worry about things like setting the environment and configuring the things manually. Applications deployed in cloud will do everything from their end and will give you a neat clean report. But for most of the organizations, due to policy or compliance reasons they don't really want to upload their data, code, and application to cloud.

For them, cloud is nothing, it's just somebody else's computer. So there comes an advantage of mobile security framework. Everything is hosted in your environment. Well in that case, you only have to set up mobile security framework in your environment once. Once it is set up, you don't have to worry about anything. So from the next time onwards just give it the APK, IPA, or the source code so that it will do the security analysis and give your report. You don't have to go through all the process of setting up your environment, configuring it, finding the correct tools, capturing the data, and then again doing the security analysis. The framework automates everything for you.




So the basic requirements to run mobile security framework (MobSF) are, if you want to do security analysis of Android application that means if you want to do security analysis of Android binaries, or source code, you need: Python 2.7, Django 1.8, Oracle Java – JDK 1.7 or higher and you need Oracle VirtualBox as well. In case of iOS application, you will need: a MacBook or a Mac device to set up mobile security framework so that it can support security analysis of iOS applications as well. Again it also requires Python 2.7, Django 1.8, Oracle Java – JDK 1.7+, Oracle VirtualBox, and as I said before, a Mac.




So here I have a picture of how static analysis functions in mobile security framework. You can provide Android binaries, iOS binaries and compressed Android or iOS source code as the input to MobSF. The mobile security framework will perform a static analysis and then give you the output. MobSF also allows you to generate a pdf report from the output. This report will contain the list of vulnerabilities identified by mobile security framework.