DeepSec2017 Workshop: Mobile App Attack – Sneha Rajguru

Posted on **October 16,2017** by **sanna**

The world's gone mobile. Mobile devices have surpassed the standard computer (i.e. desktop) installation multiple times. In turn this means that you will encounter these devices most definitely when testing or implementing security measures. Usually adversaries do not use the platform itself. They use software to gain entry. This is why mobiles apps are the most preferred way of delivering the attacks today. Understanding the finer details of mobile app attacks is soon becoming an essential skill for penetration testers as well as for the app developers & testers. This is why we have a special training for you at DeepSec 2017.

So, if you are an Android or an iOS user, a developer, a security analyst, a mobile pen-tester, or just a mobile security enthusiast the training 'Mobile App Attack' is of definite interest to you, as the course familiarizes attendees with in-depth technical explanation of some of the most notorious mobile (Android and iOS) based vulnerabilities, ways to verify and exploit them, along with various Android, iOS application analysis techniques, inbuilt security schemes and teaches how to bypass those security models on both the platforms.

With live demos using real-world vulnerable Android and iOS apps intentionally crafted by the trainer, Sneha Rajgura, attendees shall look into some of the common ways of how malicious apps bypass the security mechanisms or misuse the given permissions.

Apart from that trainees shall have a brief understanding of what is so special about the latest Android 8 and iOS 10 security and the relating flaws. The course outline is a follows:

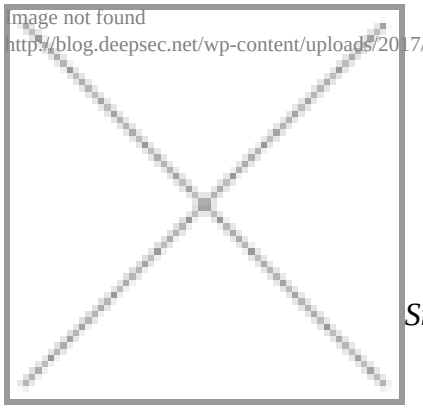
- ARM basics and Android native code.
- Reverse engineer Dex code for security analysis.
- Jailbreaking/rooting of the device and also various techniques to detect jailbreak / root access.
- Runtime analysis of the apps by active debugging.

Modifying parts of the code, where any part can be specified as some functions, classes and to perform this check or to identify the modification, you will learn how to find and calculate the checksum of the code. The objective in this section will be to learn, reverse engineering an application, get its executable binaries, modify these binaries accordingly, and re-sign the application.

Runtime modification of code – the objective is to learn how the programs/codes can be changed or modified at runtime. You will learn how to perform introspection or overriding the default behaviour of the methods during runtime, and then you will learn how to identify if the methods have been changed). For iOS you can make use of tools such as Cycript, snoop-it etc.

By the end of training, based on the course content CTF challenges written by the trainer will be launched, where the attendees will use their skills learnt in the workshop to solve the CTF challenges. The workshop will begin with a quick understanding on the architecture, file system, permissions and security model of both iOS and Android platform.

We recommend this training for anyone shepherding mobile devices or penetration testing environments where these devices get you an advantage.



Sneha works as Security Consultant with Payatu Software Labs LLP. Her areas of interest lies in web application and mobile application security and fuzzing. She has discovered various application flaws within open source applications such as PDFLite, Jobberbase, Lucidchart and more. She has spoken and provided training at GNUnify, FUDCon, DefCamp, DefCon, BSidesLV, AppSec USA and Nullcon. She is also the chapter lead for null - Pune.

Posted in:Conference,Training | Tagged:Android,Attack,DeepSec,IOS,Mobile,Mobile App,Smartphone,Training | With 0 comments