ENCIPHERS

Getting Started With Hacking Android & iOS Apps

Tools, Techniques & Resources

Abhinav Mishra

Founder, ENCIPHERS

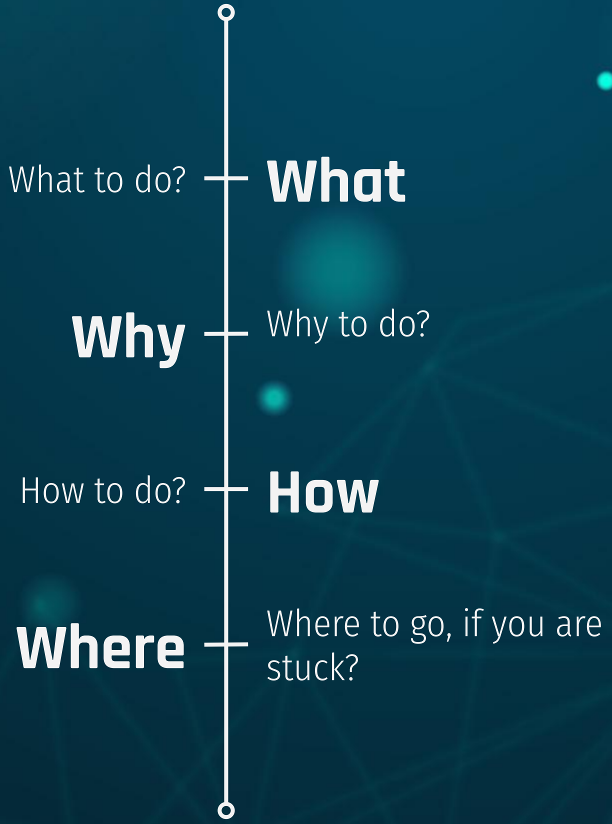
ENCIPHERS

InfoSec Consulting | Training

@enciphers_
@Octac0der

www.enciphers.com

Mobile Application Penetration Testing



What

What to do?

Why

Why to do?

How

How to do?

Where

Where to go, if you are stuck?

Disclaimer

This is a 1 hour talk. I strongly believe that in focusing on technical parts in one hour, is not the best approach.

Hence, this talk will majorly be about the methodology and discussing resources.

What to test? What to look for?

01

The methodology should be based on knowledge, not the tools

What?

The mobile application penetration testing is mainly divided in two parts:

- **Static Analysis**
  - As the name suggests, stuff that can be tested statically. Maybe even without installing the app.
- **Dynamic Analysis**
  - As the name suggests, stuff that can be tested when the app is running. Network calls, crypto, storage etc.

What?

What are the ingredients of a mobile application?

- Do you know the structure of the application package?
  - IPA | APK ~ Zip
- Manifest | Plist
- Resources that the app would need
- Source code
- XML? Config? Res? Certs etc.

What?

What happens when you install and use a mobile app?

- Permission on device?
  - To access data, use hardware, access other apps etc.
- Provide personal/account data.
  - Username/Email/Password etc.
- Network calls?
  - TLS? MITM?
- On device Security? Data at rest.
  - Crypto? Storage details
- API Security?
  - IDOR?
  - Authorisation/Authentication?

What?

Anything else on the device which:

- Handles user and application data
- Handles network connection
- Uses device permissions
- Implements a security control

Why?

Ok, so we know what all things are there to be tested/analysed. But why do we need to test each of these things?

- **Static Analysis:**
  - Sensitive information inside app package might lead to more attack surface.
  - Bad crypto implementation might be bypassed.
- **Dynamic Analysis**
  - User and application internal data should be safeguarded
  - Not implementing a security control is a security issue, bypassing it might not always be
  - Request and response is the place where all the action happens, this should be secure
  - APIs, are the biggest source of vulnerabilities in mobile applications

How?

If you know what to test and why to test, then finding or knowing how to test that might be the easiest part.

IMHO, majority of people focus only on this section...

- What tools to use?
- How to use the tools?
- Click to hack/secure applications

So, let's talk about how to do each of these....

Tools, Techniques & Resources?

What to test?

- Mobile Application Security Testing Checklist

How to test?

- Setting up lab?
  - Hardware Requirements:
    - Android:
      - Android Studio/ADB
      - Any virtual device, Genymotion, AVD & Tools
    - iOS:
      - Preferably Mac, or a high (good) config laptop
      - iDevice (iPhone, iPad etc.) [Thanks to Checkra1n]

Mobexler

Mobexler: A customised virtual machine, designed to help in penetration testing of Android & iOS applications.

When to use:

- Does not have Mac
- Don’t want to install a large amount of security tools on Mac
- Want to test Android & iOS apps at the same time, from the same setup

Let’s get to Mobexler then.

Tools, Techniques & Resources?

Tools?

- Android: https://enciphers.com/awesome-android-application-security/
- iOS: https://enciphers.com/awesome-ios-application-security/

Resources?

- Jailbreaking: https://canijailbreak.com/
- Mobile application hacker's handbook
- OWASP MSTG: https://mobile-security.gitbook.io/mobile-security-testing-guide/
- Talks on iOS & Android Security:
  - Android: https://www.youtube.com/watch?v=B3Udl86Zu20&t=20700s
  - iOS: https://www.youtube.com/watch?v=B3Udl86Zu20&t=22920s
  - Demystifying Frida: https://www.youtube.com/watch?v=kd05JjCqViY
- Blogs:
  - iOS Security: http://www.allysonomalley.com/
  - Reverse engg. iOS apps: https://github.com/ivRodriguezCA/RE-iOS-Apps
  - Android Security: https://medium.com/knowing-android/modern-security-in-android-part-1-6282bcb71e6c

Tools, Techniques & Resources?

Resources?

- Frida Cheat Sheet, for Android: https://erev0s.com/blog/frida-code-snippets-for-android/
- Android App Reverse Engg: https://maddiestone.github.io/AndroidAppRE/

Techniques:

- Jailbreak bypass in iOS: https://syrion.me/blog/ios-swift-antijailbreak-bypass-frida/
- SSL Pinning bypass: https://www.cyclon3.com/bypass-instagram-ssl-certificate-pinning-for-ios
- Xamarin cert pinning bypass: https://www.gosecure.net/blog/2020/04/06/bypassing-xamarin-certificate-pinning-on-android/
- Frida scripts: https://codeshare.frida.re/
- Frida Scripts: https://github.com/0xdea/frida-scripts

Trainings:

- iOS Application Security: https://www.enciphers-trainings.com/p/ios-application-security

(There's) no such thing as a stupid question.

Questions?

THANKS!

Do you have more questions?

a@enciphers.com
Join Slack: Invite Link

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.