Android Security & Exploitation

Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

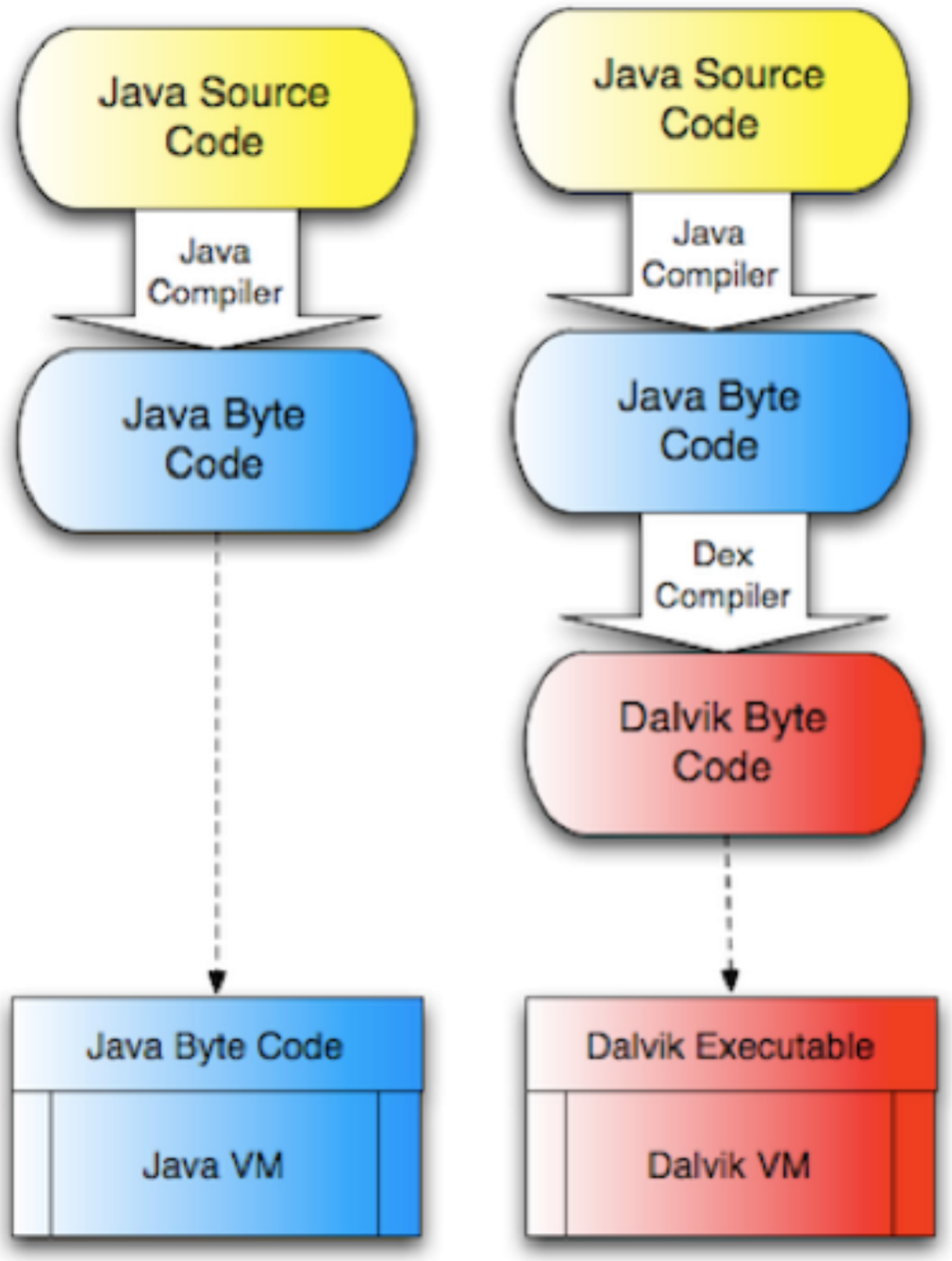
Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

Android Applications

Android Applications

- File format APK
- Archive file contains the java codes, raw files and the other resources
- Runs within a virtual machine
- Dalvik Virtual Machine executes the dex file

Android Applications



Signing in Android

- No certificate authority, unlike iOS
- Developers could generate their own certificates
- App signed with the public key, whereas the private key stays with the developer

Signing Apps in Android

- **keytool** –**genkey** –v –**keystore** [nameofkeystore] –**alias** [your_keyalias] –**keyalg** RSA –**keysize** 2048 –**validity** [numberofdays]

- **jarsigner** –verbose –**sigalg** MD5withRSA –**digestalg** SHA1 – **keystore** [name of your keystore] [your **.**apk file] [your key alias]

- **jarsigner** –verify –verbose [path-to-your-apk]

Verifying apps signature

- **MANIFEST.MF** – declares the resources
- **CERT.RSA** - Public Key Certificate
- **CERT.SF** – All the resources accounted for the app's signature
- **Printing the signatures :**
  - keytool -printcert -file META-INF/CERT.RSA
- **Signature of files included :**
  - cat META-INF/CERT.SF

```
% tree
.
├── AndroidManifest.xml
├── assets
├── libs
|   └── android-support-v4.jar
├── proguard-project.txt
├── project.properties
├── res
|   ├── drawable-hdpi
|   |   ├── ic_action_search.png
|   |   └── ic_launcher.png
|   ├── layout
|   |   └── activity_my_simple_game.xml
|   ├── menu
|   |   └── activity_my_simple_game.xml
|   ├── values
|   |   ├── dimens.xml
|   |   ├── strings.xml
|   |   └── styles.xml
|   └── values-large
|       └── dimens.xml
└── src
    └── com
        └── aditya
            └── helloworld
                ├── MySimpleGame.java
                └── myservice.java
```