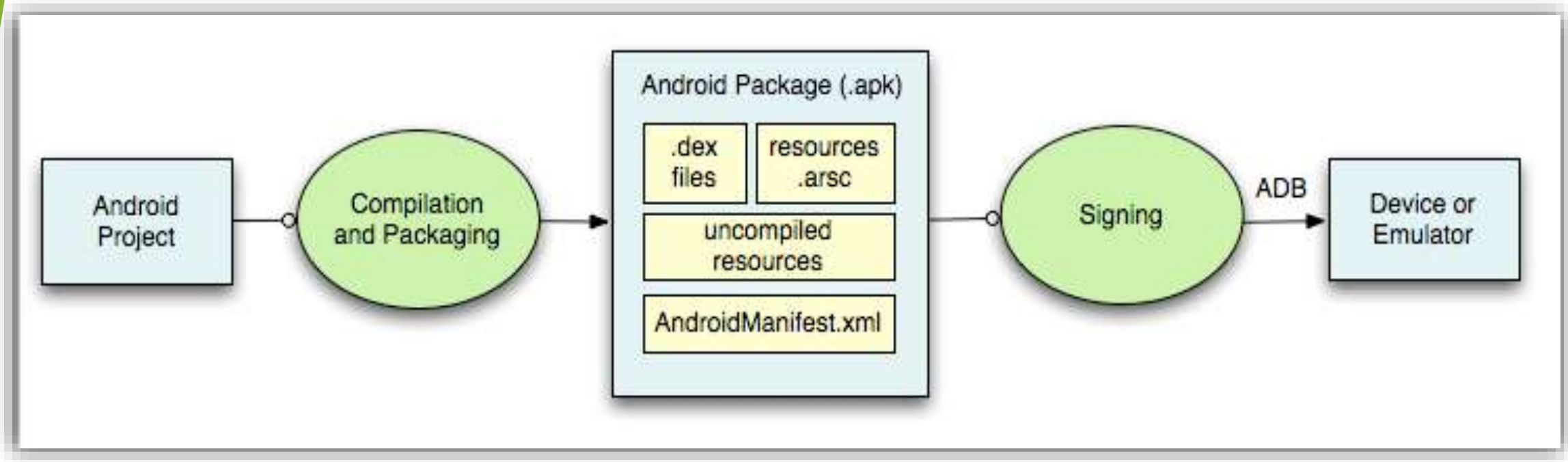
Secure Coding Guidelines

- Such guidelines even exists?
- Who cares! No one's gonna hack my app.
- Lets finish this project anyhow!!!

Secure Coding Guidelines

- Computer Emergency Response Team (CERT)
- Expert groups that handle Computer/IT security incidents.
- Issued Android Secure Coding Guidelines.
- Mission: We reduce the number of vulnerabilities to a level that can be fully mitigated in operational environments.

Packaging


Android Project
Compilation and Packaging
Android Package (.apk)
.dex files
resources .arsc
uncompiled resources
AndroidManifest.xml
Signing
ADB
Device or Emulator

Attack Vectors

in Android

Attack Vectors

Attack Vectors

- Mounting SD Card in PC
- Malicious App
- Network Attack
- Malicious File Attack
- User’s Unawareness
- USB Debugging
- Root permissions!! (Can do anything)

Security Policy

in Android

Unix Security Policy

1. Process Isolation
2. Hardware Isolation
3. User Permission Model
4. R/W/X Permissions to file
5. Secure IPC

Android Security Policy

1. Application Isolation
2. Sandbox of Application
3. Secure Communication
4. Signing the Application
5. Permission model of Application

To Do's

To Secure Apps

Avoid Simple Logics

```
private void validate(){
    if(mLoginAccess == 1 ){
        // TODO: update user.
    }
}
```

```
private void validate() {
    if (mLogin.hasAccess == true) {
        // TODO: update user.
    }
}
```

```
private void validate() {
    if (mLogin.hasAccess) {
        // TODO: update user.
    }
}
```

Test 3rd Party Libraries!

- Caution: Developers rely heavily on third-party libraries. It is important to thoroughly probe and test this as you test your code. Third-party libraries can contain vulnerabilities and weaknesses. Many developers assume third-party libraries are well-developed and tested, however, issues can and do exist in their code.

Use Encryption

- **Caution**: External storage can become unavailable if the user mounts the external storage on a computer or removes the media, and there's no security enforced upon files you save to the external storage. All applications can read and write files placed on the external storage and the user can remove them. http://developer.android.com/guide/topics/data/data-storage.html

But How to Encrypt?

To Secure Apps

How to Encrypt or Encode?

1. Encode Shared Preferences
2. Encrypt SQLite: SQLCipher
3. Encrypt Network: TLS
4. Data Encryption: Facebook's Conceal Library
5. MD5, SHA Sensitive Data

To be Secured

1. Secure Intents
2. Secure WebView
3. Secure Logs
4. Secure Intent Leaks

Code Obfuscation

1. Proguard
2. Don't include unused Classes and Libraries
3. Difficult to protect from Smali Decompilation

To Use

1. Use of Tokens for Authentication
2. Use of HTTPS!

Our Evils

1. ADB
2. Malicious Applications
3. Unprotected Network
4. Sniffers

Our Friends

1. Android Fuzzers
2. Xposed Framework
3. Drozer
4. APKtool or any other Static Analysis Tool
5. Penetration Tools for Android
6. and Many more…