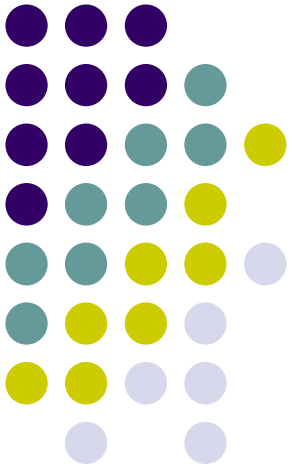
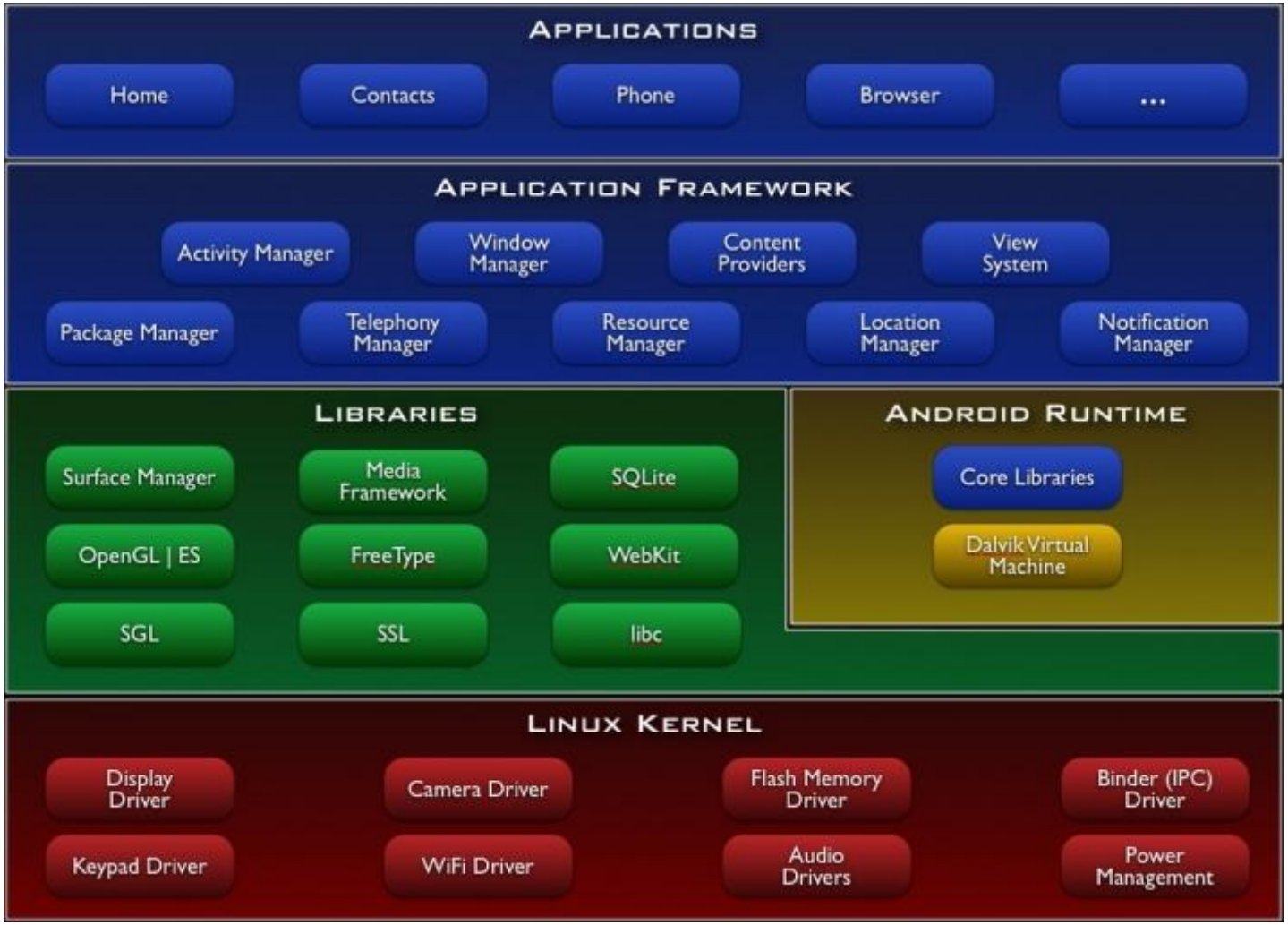
Check and detect malware in android

OMID EDRISS

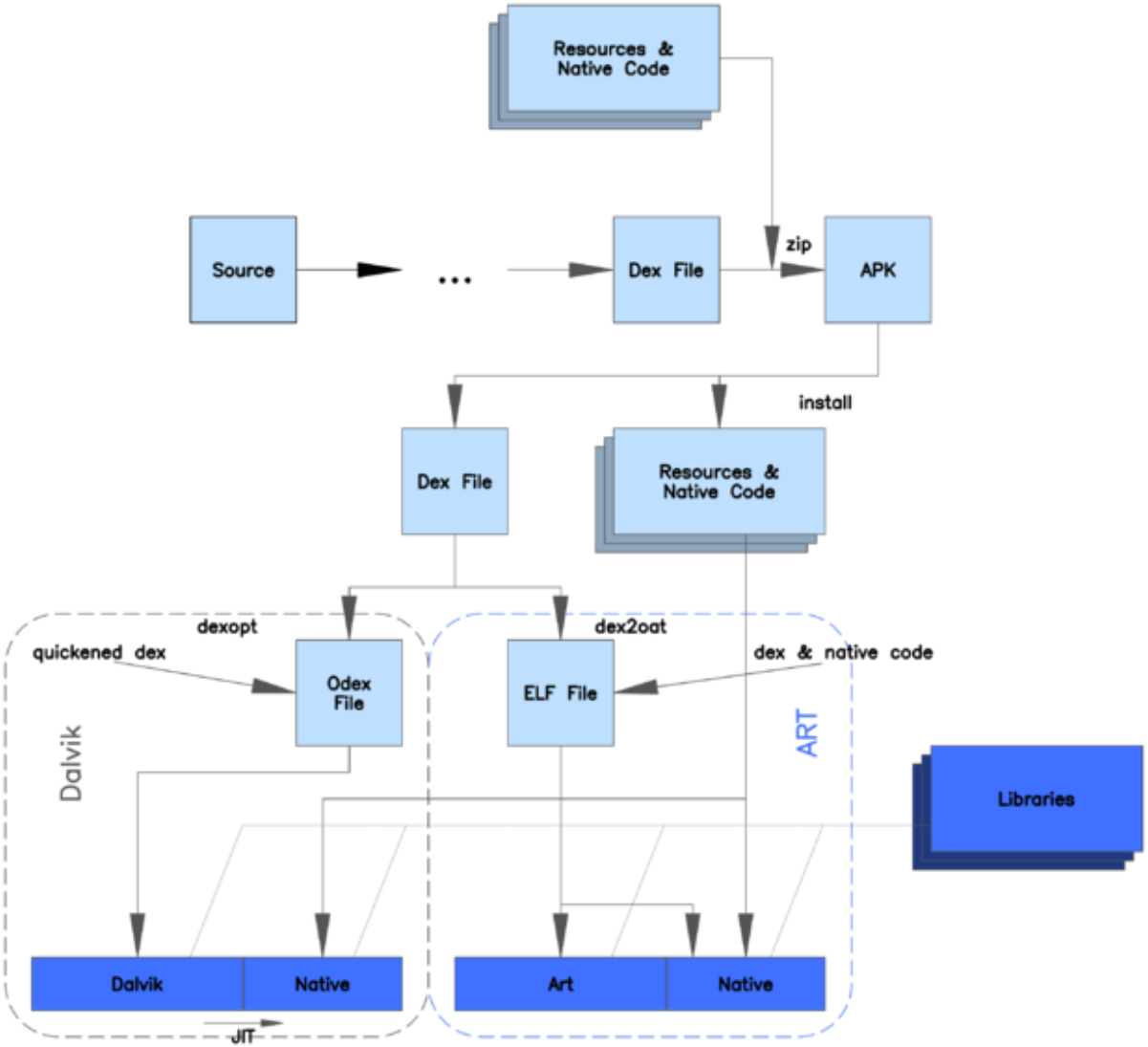


ir.linkedin.com/in/omidedriss
github.com/omidedriss

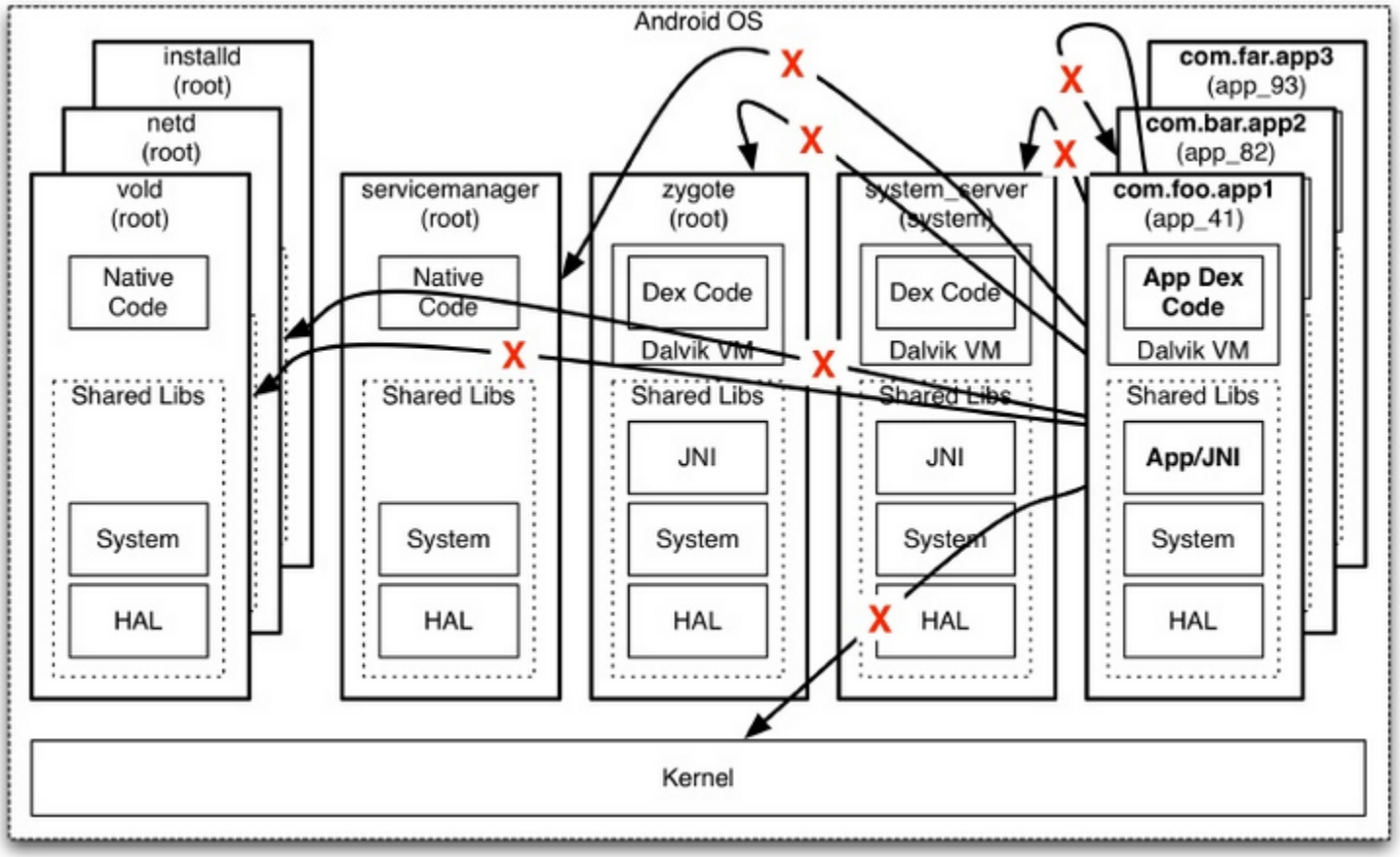
Android Architecture



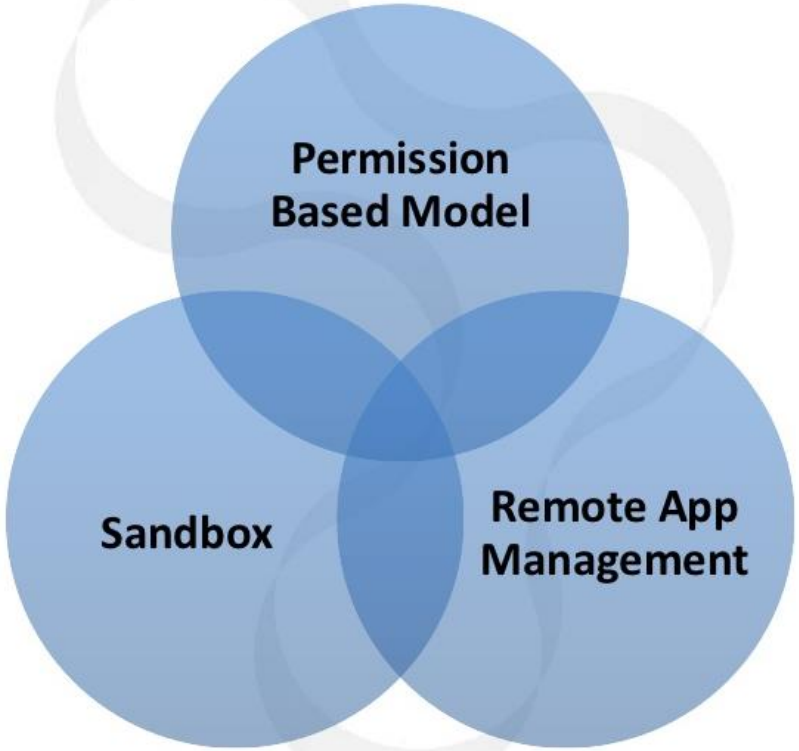
Different ART and Dalvik



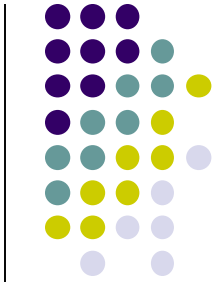
Default Android Permissions Policy



Android Security Architecture



Android Security – Permission based model



- Permission-based Model
  - Linux + Android's Permission
  - Well defined at system level
  - Approved by user at install
  - High-level permissions restricted by Android runtime framework
  - For example, an application that needs to monitor incoming SMS messages would specify

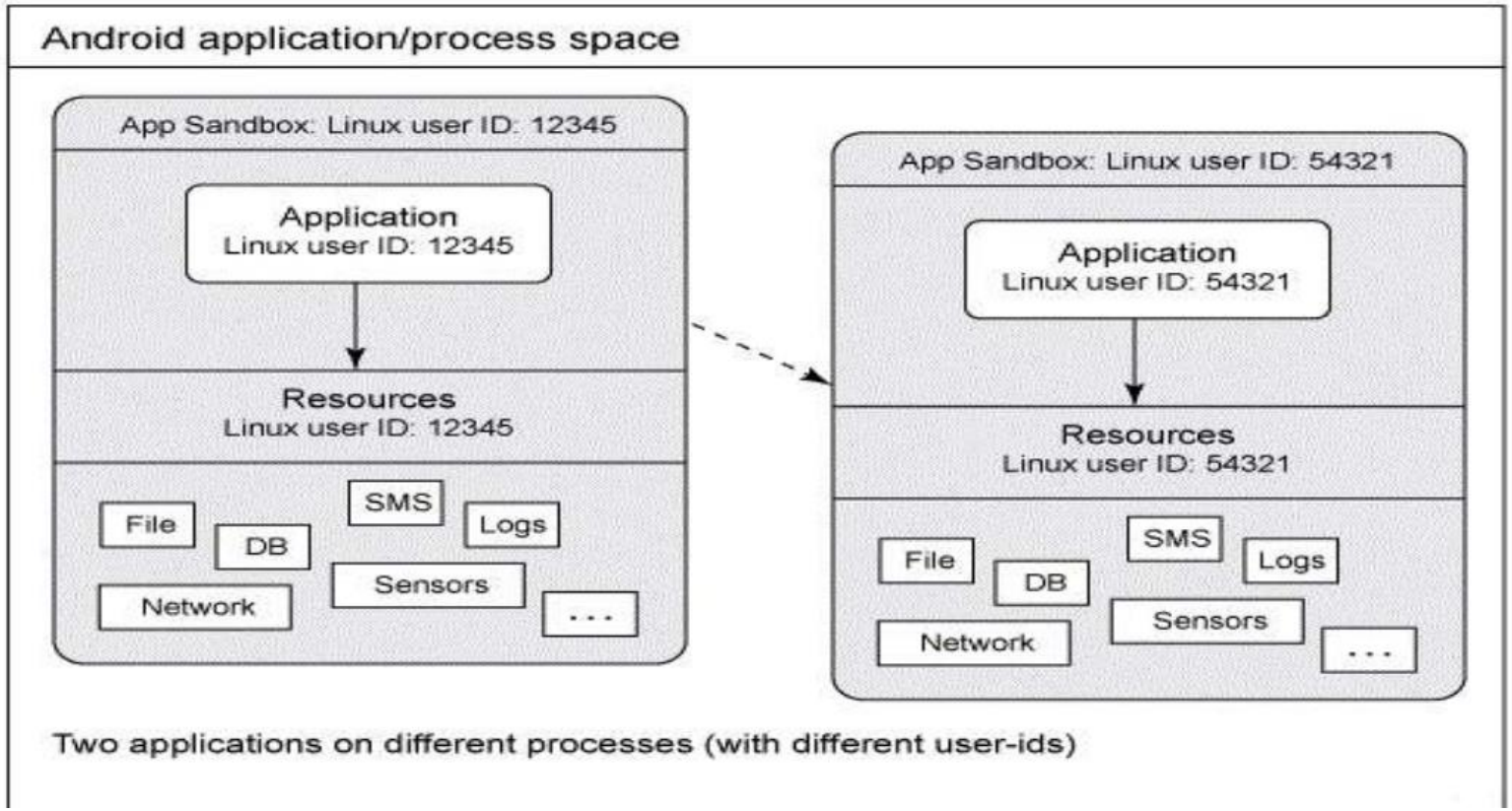
```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.android.app.myapp" >
  <uses-permission android:name="android.permission.RECEIVE_SMS" />
    ...</manifest>
```

Android Security – Remote App Management

- Remote Install/removal
  - Google can remove or install apps remotely
  - Users can install apps remotely from online Android Market

http://market.android.com

Android Security - Sandbox



Malware detection techniques

- Static
- Dynamic

Dynamic Analysis

- system calls
- network access
- Files
- memory modifications

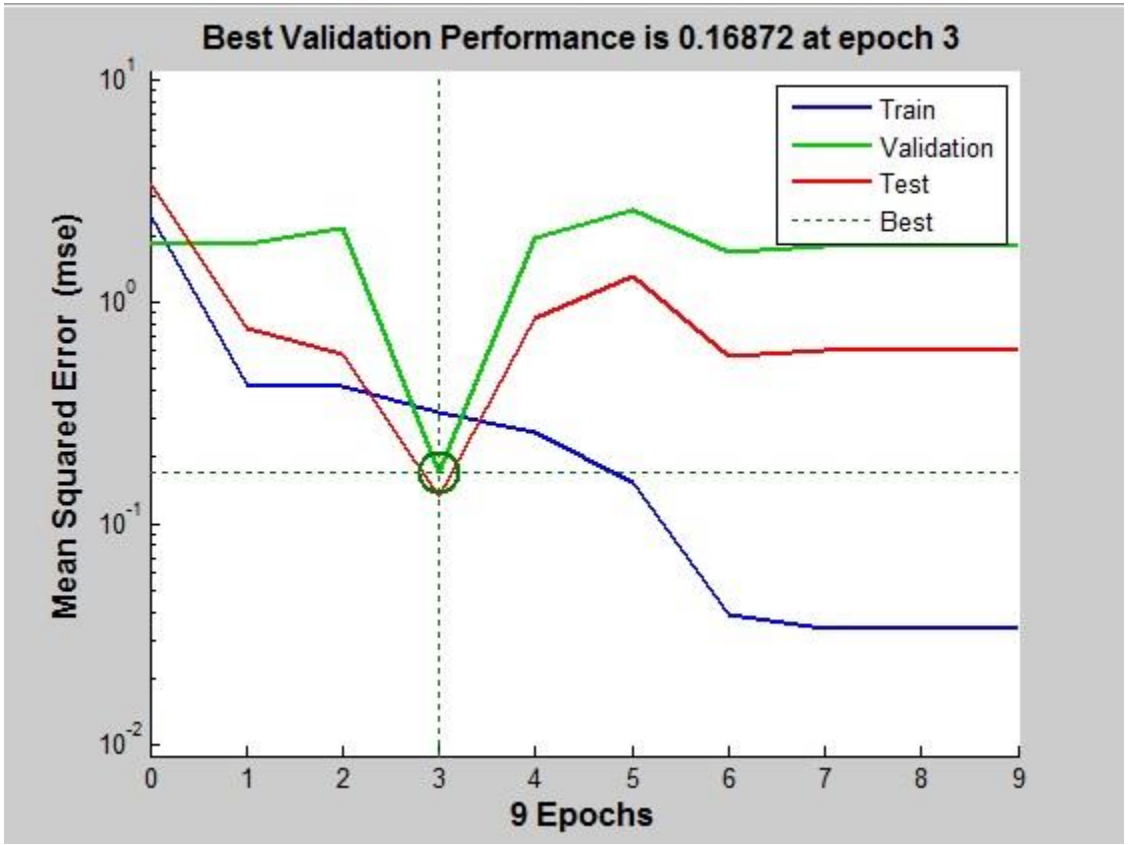
Creating the dataset

- Read File system * time variance
- Write file system * time variance
- Open network
- Service gm & mms

Detection method with MLP

- Learning
- Validation
- test

Conclusion


Best Validation Performance is 0.16872 at epoch 3
Mean Squared Error (mse)
9 Epochs
Train
Validation
Test
Best
10^1
10^0
10^-1
10^-2
0
1
2
3
4
5
6
7
8
9