**5.1 REVERESE ENGINEERING AND MALWARE ANALYSIS**

Shubhash s

Roopkatha pradhan

Gitesh bhavsar

Shreya dokania

**REVERSING MOBILE APPLICATION**

We took a simple mobile application which will print whether the given user is VIP user or not. In this application there is only one VIP user whose username is “sabin”. We going to reverse engineer it and make it available for everyone.

“Dex-2-jar” is a opensource tool to covert Dex file into jar file.

A screenshot of a computer

Description automatically generated

A picture containing text, screenshot, font

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

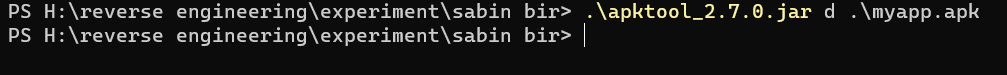
Viewing the jar file in JD decompiler which only readable not writeable

A screenshot of a computer

Description automatically generated with medium confidence

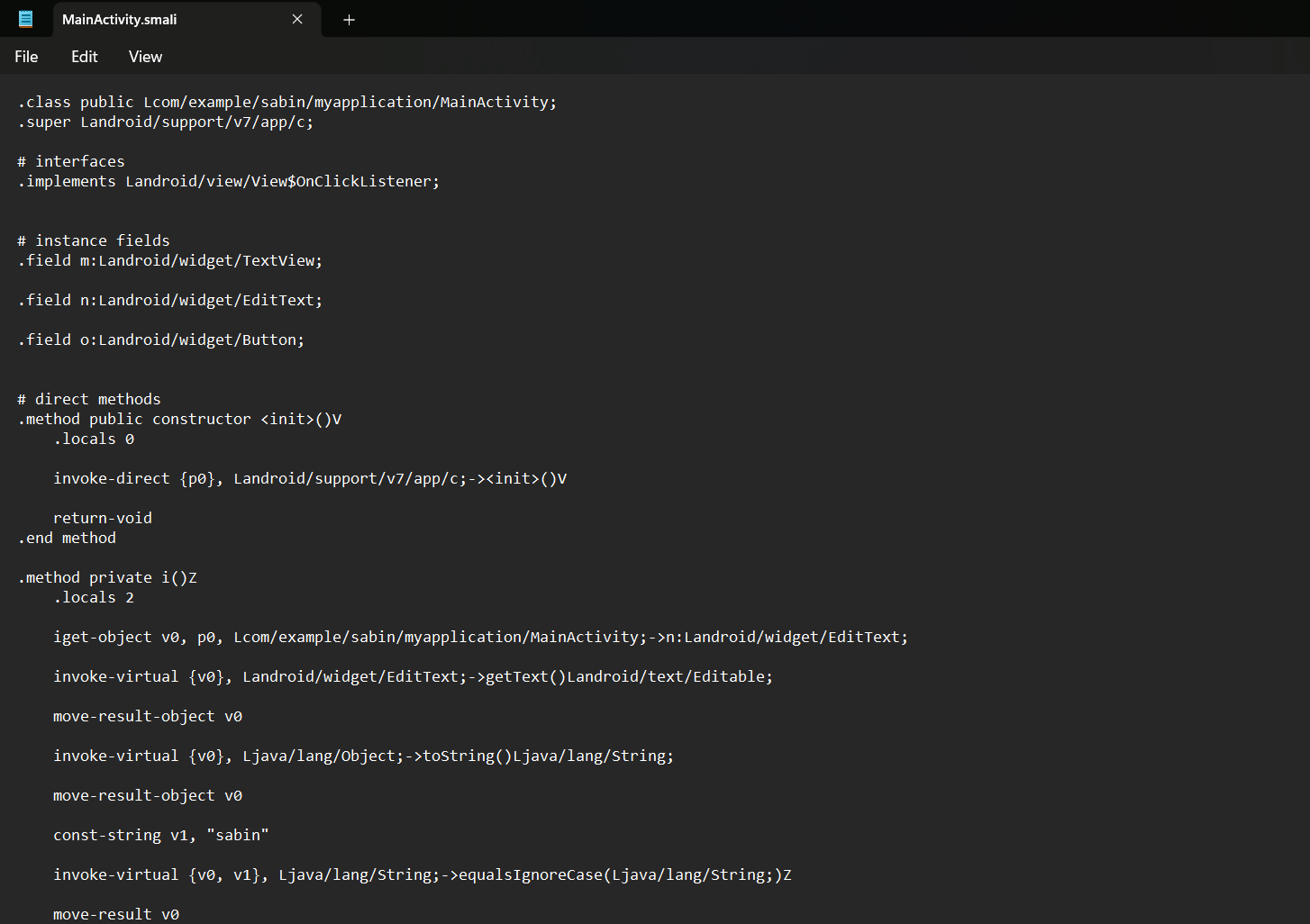
In this code we have to change the return value in the Boolean i() function so that it always return true so that everyone is VIP user.

To modify reversed code we need to use apktool

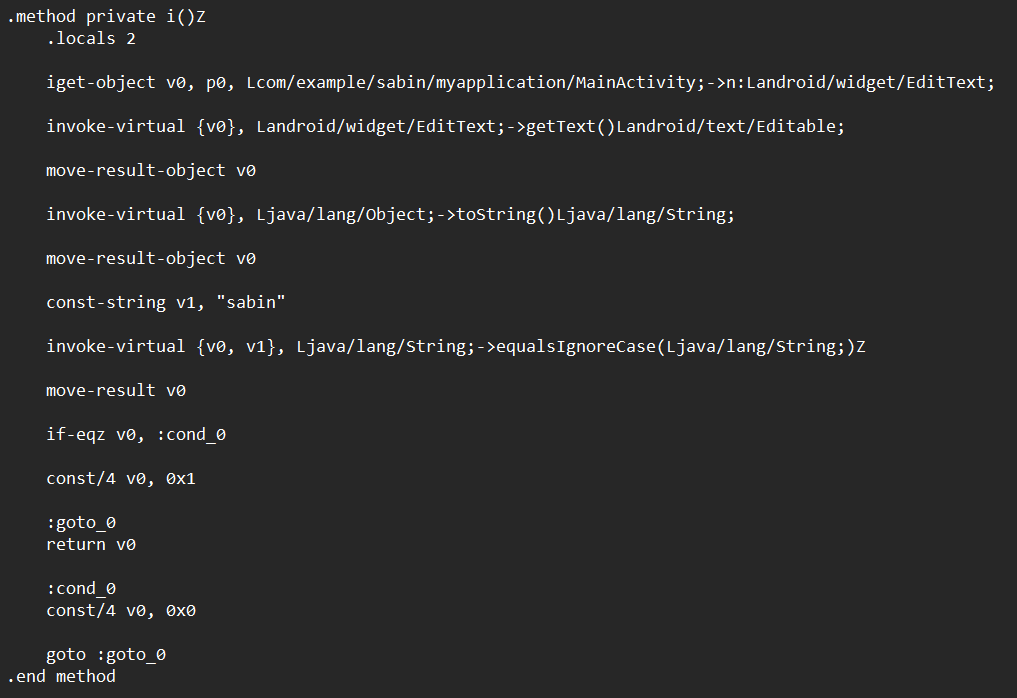


A screenshot of a computer

Description automatically generated



In this reversed code we found the i() function

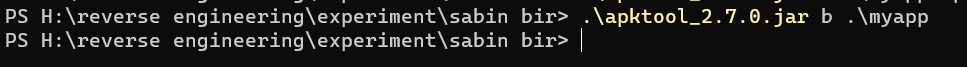


At bottom we found the if-else statement and the variable “V0” is used to return the true/false. So we need to change it as 1 which is always true.

A screen shot of a computer program

Description automatically generated with low confidence

Now we have made the APK with our modified code



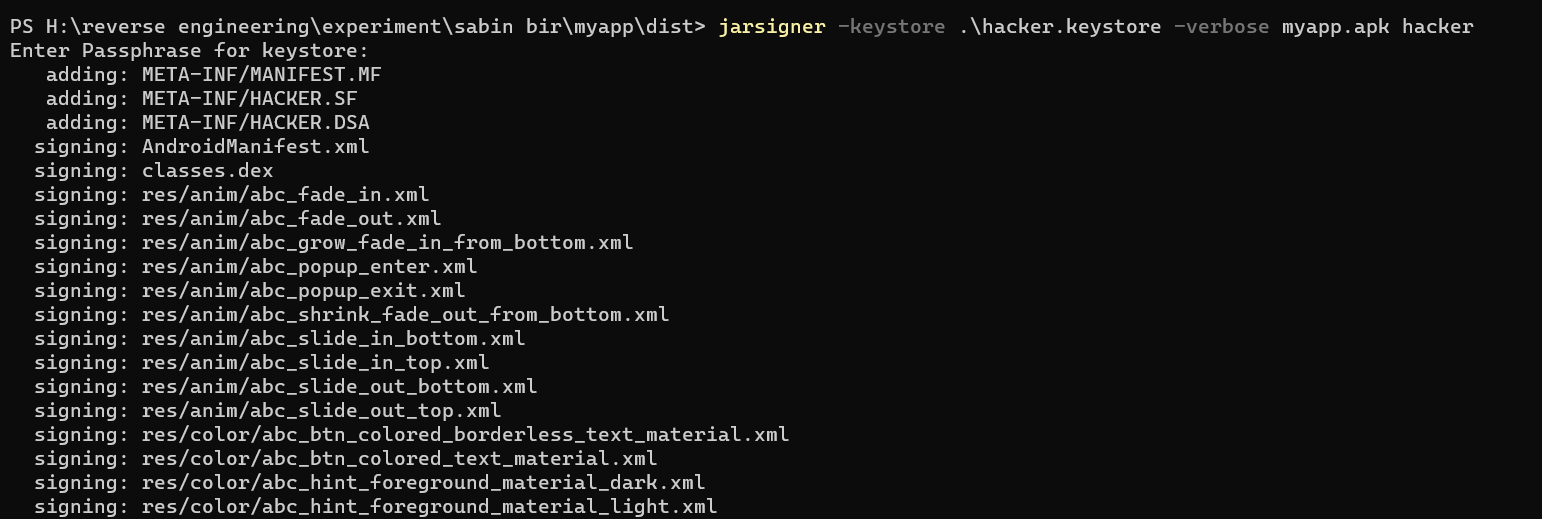
A screenshot of a computer

Description automatically generated with medium confidence

Now final step we need to sign the APK using keytool and jarsigner,

A screen shot of a computer

Description automatically generated with medium confidence



A computer screen with white text

Description automatically generated with low confidence

**CONCLUSION:**

We have successfully reverse engineered and modified the app now every user is VIP user.