Reversing the crackme0 of Lohan

Some info

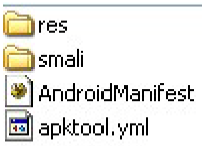
Crackme: crackme0
Autor of crackme: Lohan
Autor of manual: deurus
Dificulty: 1/10
Date: 31/10/2010

Tools used/needed

ART (Android Reverse tools)
Ultraedit 16.20.0.1011 with smali.uew wordfile
Android emulator or your phone

Introduction

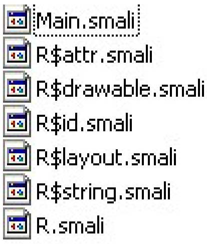
*First install ultraedit and copy the file **smali.uew** to the ultraedit's wordfiles directory. By default the directory is: C:\program files\IDM Computer Solutions\UltraEdit\wordfiles.*
Ok, now decompile it with ART. Once decompiled, explore the files, should be like this:



```
res
smali
AndroidManifest
apktool.yml
```

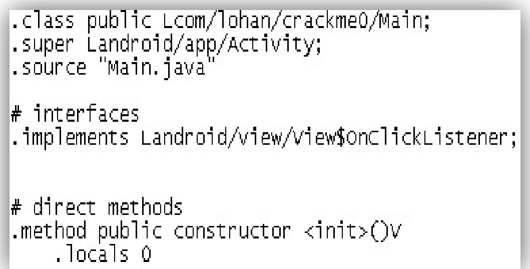
Res directory contains the icons and many xml interesting files
Smali directory contains the code
AndroidManifest.xml is the main xml file
Apktool.yml

*Go to the **\smali\com\lohan\crackme0** directory, here are this files.*



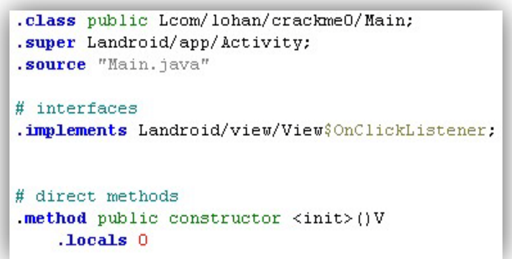
```
Main.smali
R$attr.smali
R$drawable.smali
R$id.smali
R$layout.smali
R$string.smali
R.smali
```

*The R$.... files we ignore for the moment, then open with ultraedit the **Main.smali** file.*



```
.class public Lcom/lohan/crackme0/Main;
.super Landroid/app/Activity;
.source "Main.java"

# interfaces
.implements Landroid/view/View$OnClickListener;


# direct methods
.method public constructor <init>()V
    .locals 0
```

Without smali.uew file

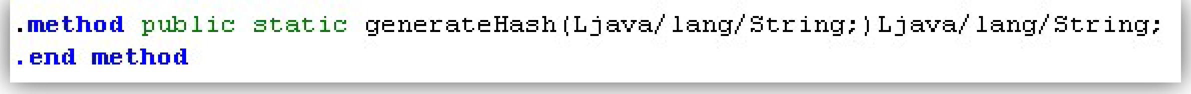


```
.class public Lcom/lohan/crackme0/Main;
.super Landroid/app/Activity;
.source "Main.java"

# interfaces
.implements Landroid/view/View$OnClickListener;


# direct methods
.method public constructor <init>()V
    .locals 0
```

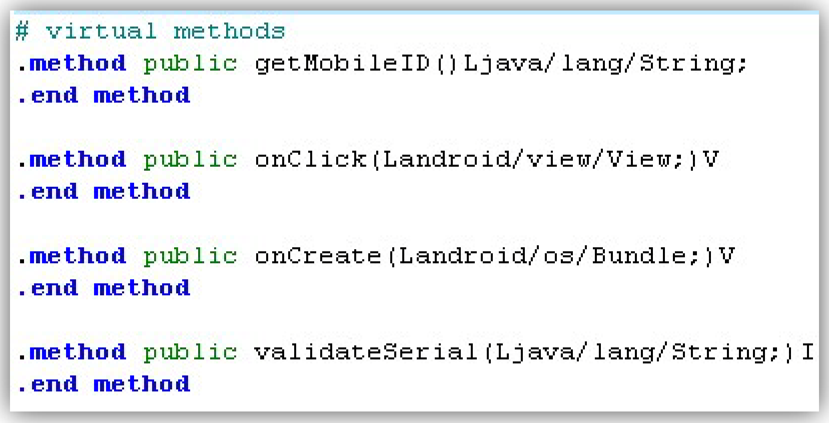
with smali.uew file

Analyzing the code

Open the file and instantly we view four interesting virtual methods and direct one



```
.method public static generateHash(Ljava/lang/String;)Ljava/lang/String;
.end method
```



```
# virtual methods
.method public getMobileID()Ljava/lang/String;
.end method

.method public onClick(Landroid/view/View;)V
.end method

.method public onCreate(Landroid/os/Bundle;)V
.end method

.method public validateSerial(Ljava/lang/String;)I
.end method
```

generateHash – hopefully it will generate a common hash

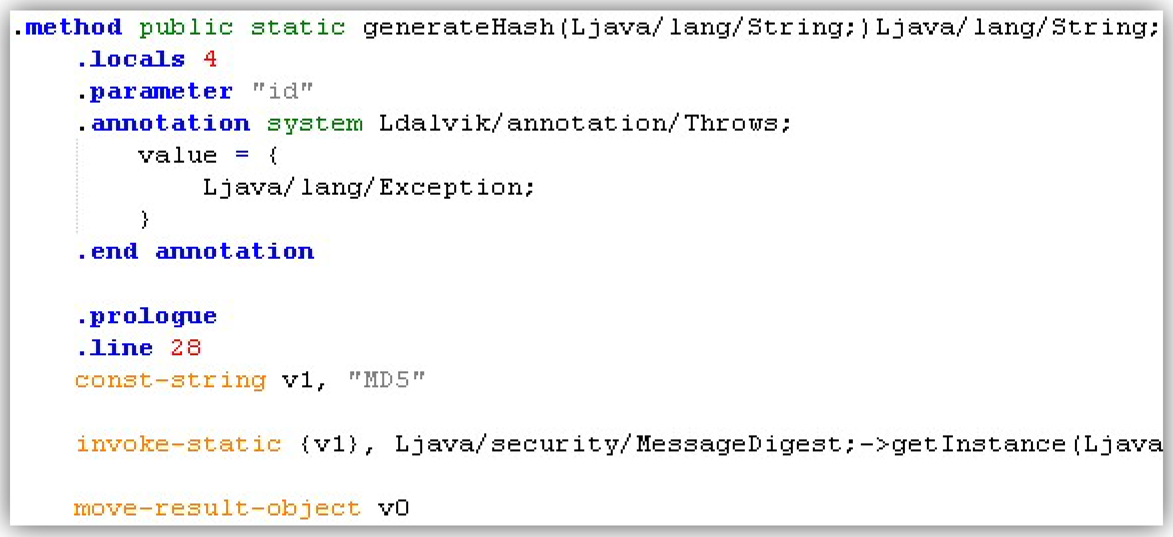
getMobileID – possibly take some info of the phone

onClick – The onClick event

onCreate – Load event

validateSerial – Is obviously :-)

Go to analize the generateHash event



```
.method public static generateHash(Ljava/lang/String;)Ljava/lang/String;
    .locals 4
    .parameter "id"
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Ljava/lang/Exception;
        }
    .end annotation

    .prologue
    .line 28
    const-string v1, "MD5"

    invoke-static {v1}, Ljava/security/MessageDigest;->getInstance(Ljava

    move-result-object v0
```

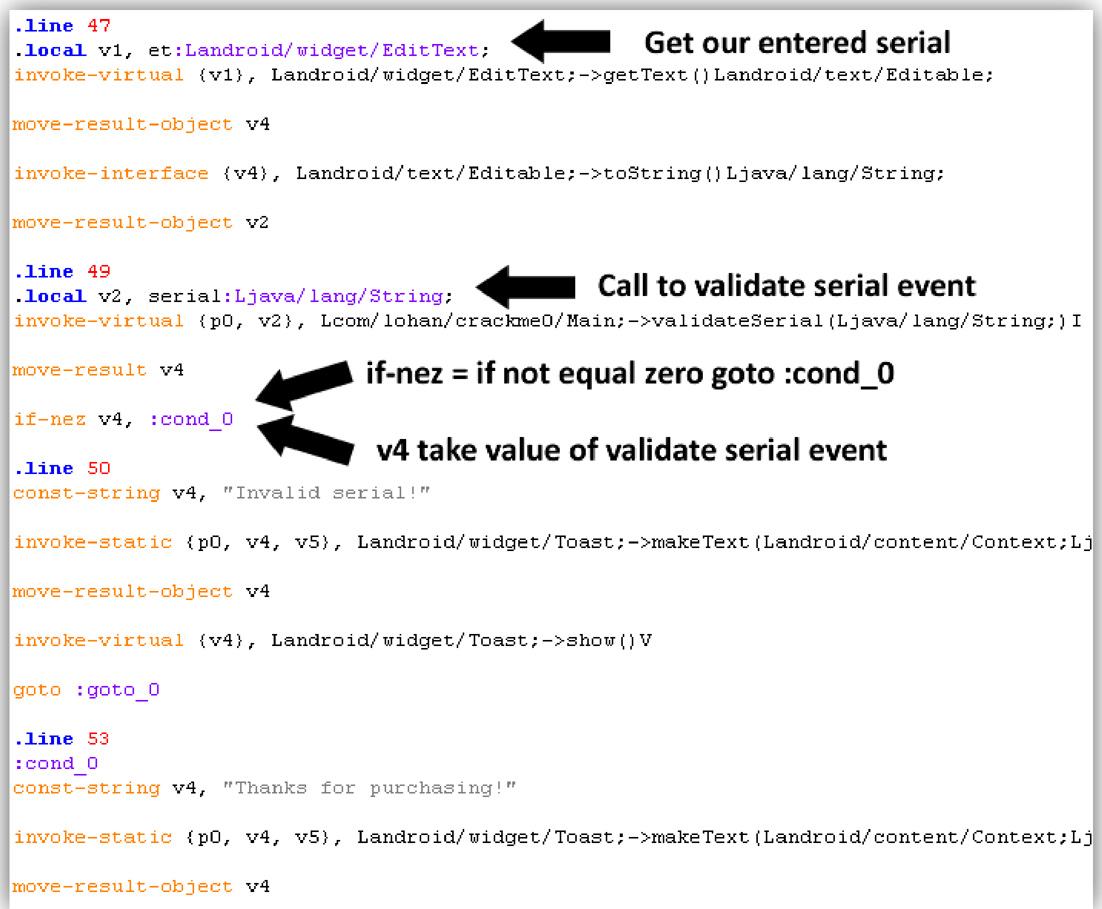
We are lucky, the hash is MD5

Go to analize the getMobileID event

```
.line 38
.local v1, mTelephonyMgr:Landroid/telephony/TelephonyManager;
invoke-virtual {v1}, Landroid/telephony/TelephonyManager;->getDeviceId()Ljava/lang/String;

move-result-object v0
```

Looking for in the android developer reference, we view that the getDeviceId() function returns the phone´s IMEI.

Go to analize the onClick event



```
.line 47
.local v1, et:Landroid/widget/EditText;
invoke-virtual {v1}, Landroid/widget/EditText;->getText()Landroid/text/Editable;

move-result-object v4

invoke-interface {v4}, Landroid/text/Editable;->toString()Ljava/lang/String;

move-result-object v2

.line 49
.local v2, serial:Ljava/lang/String;
invoke-virtual {p0, v2}, Lcom/lohan/crackme0/Main;->validateSerial(Ljava/lang/String;)I

move-result v4

if-nez v4, :cond_0

.line 50
const-string v4, "Invalid serial!"

invoke-static {p0, v4, v5}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Lj

move-result-object v4

invoke-virtual {v4}, Landroid/widget/Toast;->show()V

goto :goto_0

.line 53
:cond_0
const-string v4, "Thanks for purchasing!"

invoke-static {p0, v4, v5}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Lj

move-result-object v4
```

Get our entered serial

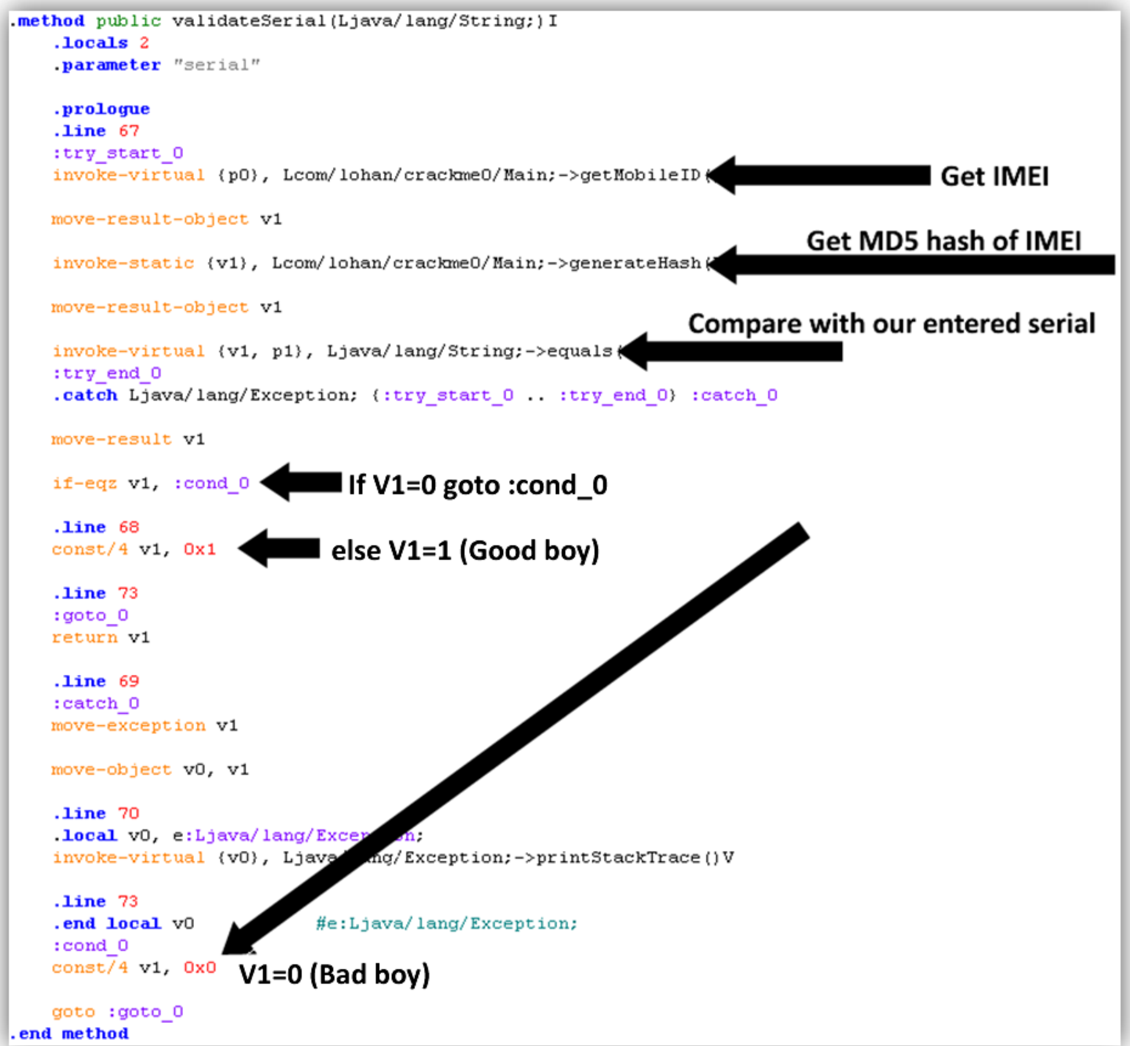
Call to validate serial event

if-nez = if not equal zero goto :cond_0

v4 take value of validate serial event

*Here we can to patch the check routine simply change **if-nez** by **if-eqz**, only with this change the victim is patched. But we follow.*

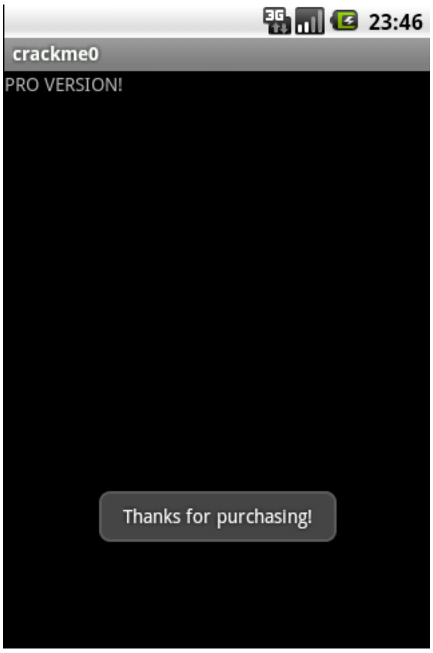
Go to analize the validateSerial event



```
.method public validateSerial(Ljava/lang/String;)I
    .locals 2
    .parameter "serial"

    .prologue
    .line 67
    :try_start_0
    invoke-virtual {p0}, Lcom/lohan/crackme0/Main;->getMobileID(

    move-result-object v1

    invoke-static {v1}, Lcom/lohan/crackme0/Main;->generateHash(

    move-result-object v1

    invoke-virtual {v1, p1}, Ljava/lang/String;->equals(
    :try_end_0
    .catch Ljava/lang/Exception; {:try_start_0 .. :try_end_0} :catch_0

    move-result v1

    if-eqz v1, :cond_0

    .line 68
    const/4 v1, 0x1

    .line 73
    :goto_0
    return v1

    .line 69
    :catch_0
    move-exception v1

    move-object v0, v1

    .line 70
    .local v0, e:Ljava/lang/Exception;
    invoke-virtual {v0}, Ljava/lang/Exception;->printStackTrace()V

    .line 73
    .end local v0           #e:Ljava/lang/Exception;
    :cond_0
    const/4 v1, 0x0

    goto :goto_0
.end method
```

The routine is:
Get IMEI -> MD5 hash IMEI -> Compare with our serial

Testing in the emulator/phone we can to try our theory.
I test in emulator, and in the emulator the IMEI = 000000000000000 (15 digits)



crackme0

PRO VERSION!

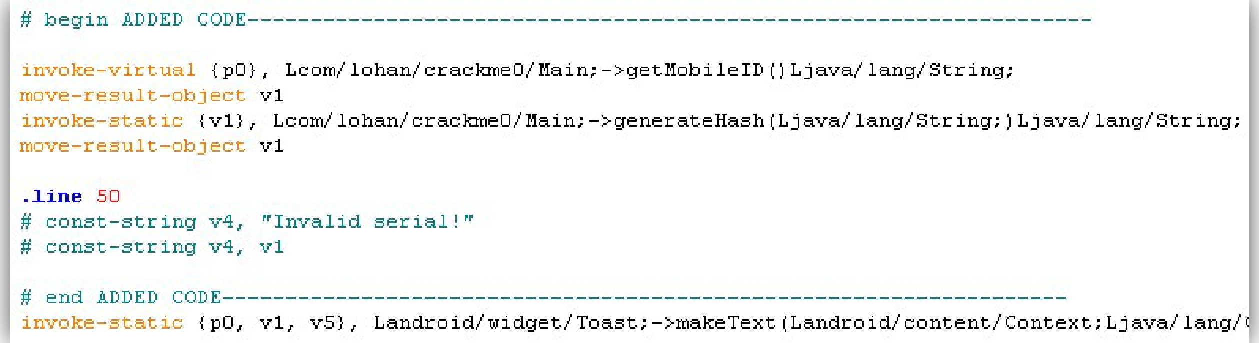
Thanks for purchasing!

Testing

IMEI = 000000000000000
MD5 hash = 5284047f4ffb4e04824a2fd1d1f0cd62

My modification

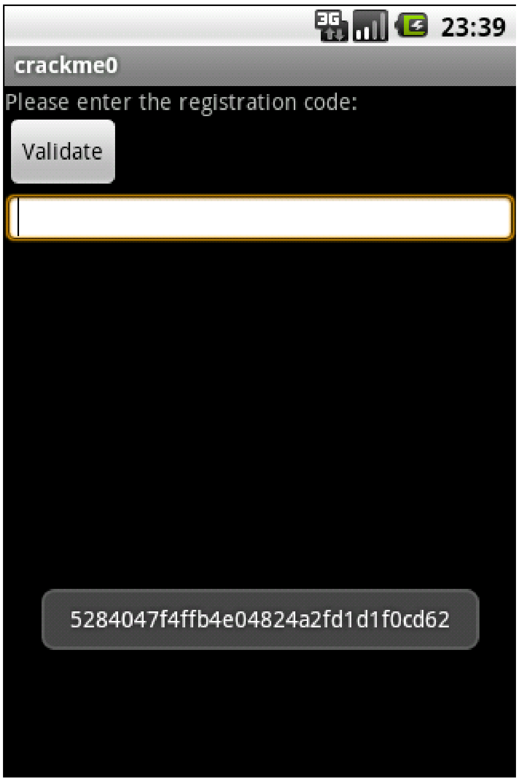
As a key generator, I modified the file to output valid serial number instead of the "Invalid serial" message



```
# begin ADDED CODE---------------------------------------------------------------------

invoke-virtual {p0}, Lcom/lohan/crackme0/Main;->getMobileID()Ljava/lang/String;
move-result-object v1
invoke-static {v1}, Lcom/lohan/crackme0/Main;->generateHash(Ljava/lang/String;)Ljava/lang/String;
move-result-object v1

.line 50
# const-string v4, "Invalid serial!"
# const-string v4, v1

# end ADDED CODE-----------------------------------------------------------------------
invoke-static {p0, v1, v5}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/
```

Get the IMEI -> Gen the hash and store in V1 -> Void the Invalid serial message

The result



Please enter the registration code:

5284047f4ffb4e04824a2fd1d1f0cd62

Links

Android developer reference
http://developer.android.com/reference/packages.html

Dalvik opcodes
http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html

made in Basque Country