

Ciberseguridad en  
dispositivos móviles

# Práctica 2

---

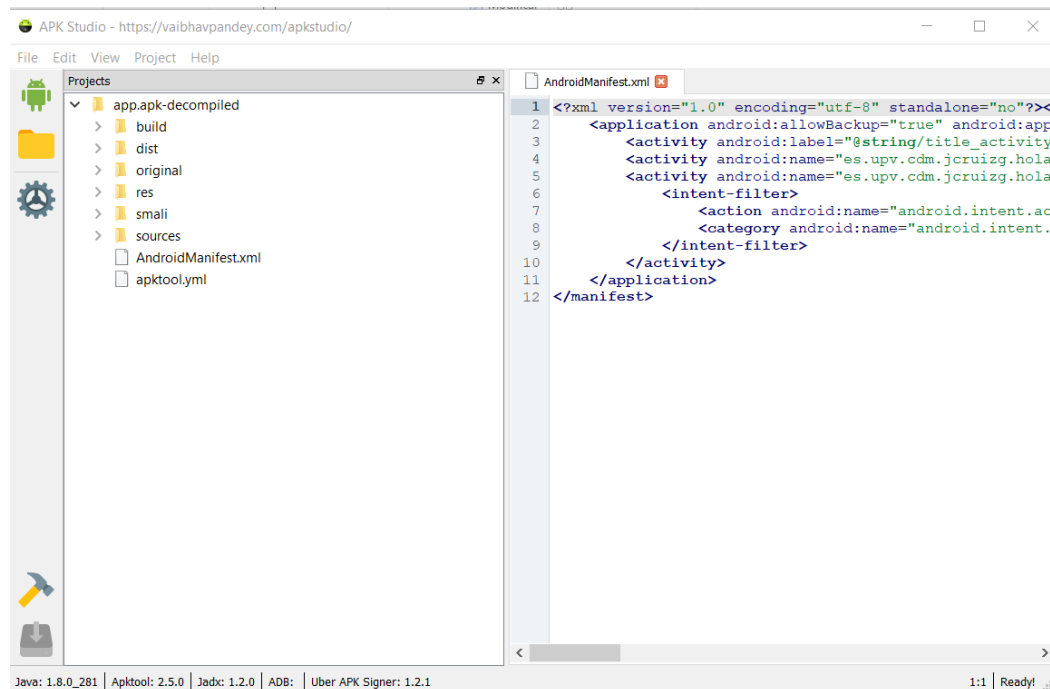
Luis López Cuerva  
Pablo Alcarria Lozano

## Introducción

El conjunto de prácticas de la asignatura “Ciberseguridad en Dispositivos móviles” la estamos realizando en conjunto Luis López Cuerva y Pablo Alcarria Lozano. Esta segunda práctica trata del desensamblado y reensamblado de aplicaciones Android.

## Resolución

Para la realización de la práctica hemos seguido los pasos propuestos, en primer lugar hemos configurado Apktool para desensamblar la app InsecureBankv2



A continuación analizamos el código en busca del mejor archivo para realizar el heurístico de evasión. Lo encontramos en el archivo MainActivity\$1.smali, concretamente en una zona dónde el programa identificaba si estábamos en un dispositivo real o uno emulado. Aprovechamos este código existente en la aplicación para crear el heurístico de evasión en el que según si el dispositivo en el que se ejecuta la aplicación es real o emulado tiene un comportamiento u otro.

```
if-eqz p1, :cond_0

const-string p1, "[MainActivity]"

const-string v0, "Ejecutas el c\u00f3digo en un emulador"

const-class v2, Les/upv/cdm/jcruizg/holamundo/LoginActivity;

.line 31
invoke-static {p1, v0}, Landroid/util/Log;->i(Ljava/lang/String;Ljava/lang/String;)I

goto :goto_0

:cond_0
const-string p1, "[MainActivity]"

const-string v0, "Ejecutas el c\u00f3digo en un dispositivo real"

const-class v2, Les/upv/cdm/jcruizg/holamundo/SegundaActividad;

.line 35
invoke-static {p1, v0}, Landroid/util/Log;->i(Ljava/lang/String;Ljava/lang/String;)I

:goto_0
iget-object p1, p0, Les/upv/cdm/jcruizg/holamundo/MainActivity$1;->this$0:Les/upv/cdm/jcruizg/holamundo/MainActivity;

new-instance v0, Landroid/content/Intent;

invoke-virtual {p1}, Les/upv/cdm/jcruizg/holamundo/MainActivity;->getApplicationContext()Landroid/content/Context;

move-result-object v1

invoke-direct {v0, v1, v2}, Landroid/content/Intent;-><init>(Landroid/content/Context;Ljava/lang/Class;)V
```

Una vez realizada esta modificación creamos el toast con el mensaje "¡¡¡ Te he hackeado !!!" en el mismo archivo. El contenido completo y modificado del archivo MainActivity\$1.smali se puede encontrar en el anexo.

```
const-string v0, "¡¡¡ Te he hackeado !!!"

const/4 v1, 0x1

invoke-static {p1, v0, v1}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequence;I)Landroid/widget/Toast;

move-result-object p1

invoke-virtual {p1}, Landroid/widget/Toast;->show()V
```

Por último se ha reensamblado y firmado la aplicación usando apktool.

## Anexo

```
.class Les/upv/cdm/jcruizg/holamundo/MainActivity$1;

.super Ljava/lang/Object;

.source "MainActivity.java"

# interfaces

.implements Landroid/view/View$OnClickListener;

# annotations

.annotation system Ldalvik/annotation/EnclosingMethod;
    value = Les/upv/cdm/jcruizg/holamundo/MainActivity;->onCreate(Landroid/os/Bundle;)V
.end annotation

.annotation system Ldalvik/annotation/InnerClass;
    accessFlags = 0x0
    name = null
.end annotation

# instance fields

.field final synthetic this$0:Les/upv/cdm/jcruizg/holamundo/MainActivity;

# direct methods

.method constructor <init>(Les/upv/cdm/jcruizg/holamundo/MainActivity;)V
    .locals 0

    .line 22

    iput-object p1, p0,
Les/upv/cdm/jcruizg/holamundo/MainActivity$1;->this$0:Les/upv/cdm/jcruizg/holamundo/MainAct
ivity;
```

```
invoke-direct {p0}, Ljava/lang/Object; -> <init>()V
return-void
.end method
# virtual methods
.method public onClick(Landroid/view/View;)V
    .locals 3
    .line 26
    iget-object p1, p0,
Les/upv/cdm/jcruizg/holamundo/MainActivity$1; -> this$0: Les/upv/cdm/jcruizg/holamundo/MainAct
ivity;
    new-instance v0, Landroid/content/Intent;
    invoke-virtual {p1},
Les/upv/cdm/jcruizg/holamundo/MainActivity; -> getApplicationContext()Landroid/content/Context;
    move-result-object v1
    const-class v2, Les/upv/cdm/jcruizg/holamundo/LoginActivity;
    invoke-direct {v0, v1, v2},
Landroid/content/Intent; -> <init>(Landroid/content/Context;Ljava/lang/Class;)V
    invoke-virtual {p1, v0},
Les/upv/cdm/jcruizg/holamundo/MainActivity; -> startActivity(Landroid/content/Intent;)V
    .line 28
    sget-object p1, Landroid/os/Build; -> DEVICE:Ljava/lang/String;
    const-string v0, "generic"
    .line 29
    invoke-virtual {p1, v0}, Ljava/lang/String; -> contains(Ljava/lang/CharSequence;)Z
    move-result p1
```

```
if-eqz p1, :cond_0

const-string p1, "[MainActivity]"

const-string v0, "Ejecutas el código en un emulador"

const-class v2, Les/upv/cdm/jcruizg/holamundo/LoginActivity;

.line 31

invoke-static {p1, v0}, Landroid/util/Log;.>i(Ljava/lang/String;Ljava/lang/String;)I

goto :goto_0

:cond_0

const-string p1, "[MainActivity]"

const-string v0, "Ejecutas el código en un dispositivo real"

const-class v2, Les/upv/cdm/jcruizg/holamundo/SegundaActividad;

.line 35

invoke-static {p1, v0}, Landroid/util/Log;.>i(Ljava/lang/String;Ljava/lang/String;)I

:goto_0

iget-object p1, p0,
Les/upv/cdm/jcruizg/holamundo/MainActivity$1;.>this$0:Les/upv/cdm/jcruizg/holamundo/MainAct
ivity;


new-instance v0, Landroid/content/Intent;

invoke-virtual {p1},
Les/upv/cdm/jcruizg/holamundo/MainActivity;.>getApplicationContext()Landroid/content/Context;

move-result-object v1

invoke-direct {v0, v1, v2},
Landroid/content/Intent;.><init>(Landroid/content/Context;Ljava/lang/Class;)V

invoke-virtual {p1, v0},
Les/upv/cdm/jcruizg/holamundo/MainActivity;.>startActivity(Landroid/content/Intent;)V
```



```
#  
  
    const-string v0, "¡¡¡ Te he hackeado !!!"  
  
    const/4 v1, 0x1  
  
    invoke-static {p1, v0, v1},  
    Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequence;I)Landroid  
    /widget/Toast;  
  
    move-result-object p1  
  
    invoke-virtual {p1}, Landroid/widget/Toast;->show()V  
  
#  
  
    return-void  
  
.end method
```