OWASP
Open Web Application
Security Project

Patching Android Binaries

OWASP Orlando 10/25/2018

Adrian Pastor

General Process

- Decompile

```
$ apktool d app.apk
```

- Analyze

`grep`, `find`, `less`, etc.

- Mod

`vi`

- Compile

```
$ apktool b app/
```

- Sign

```
$ jarsigner -verbose -keystore ~/.android/
debug.keystore -storepass android -keypass android
app/dist/app.apk androiddebugkey
```

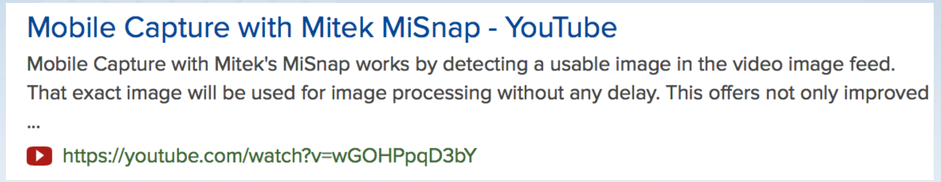
Scenario

Can’t take screenshot due to security policy.

Patching meth: tautology

app/smali/com/miteksystems/misnap/a/h.smali

```
[…SNIP…]

  invoke-virtual {p3}, Lcom/miteksystems/misnap/params/ParameterManager;->getmAllowScreenshots()I

  move-result p1

  if-nez p1, :cond_0

  if-eqz p1, :cond_0 #skip to :cond_0 "successful" patch but wrong functionality targeted

  sget p1, Landroid/os/Build$VERSION;->SDK_INT:I

  const/16 p2, 0x11

  if-lt p1, p2, :cond_0

  invoke-virtual {p0, v0}, Lcom/miteksystems/misnap/a/h;->setSecure(Z)V

  :cond_0
  return-void
```



Patching meth: tautology

app/smali/com/acme/library/core/CoreActivity.smali

```
.method protected onCreate(Landroid/os/Bundle;)V
   […SNIP…]

   iget-boolean v0, v0, Lcom/app/library/core/config/CoreConfig;->allowScreenshots:Z

   if-nez v0, :cond_1

   if-eqz v0, :cond_1 #skip to :cond_1 (successful patch)

   .line 44
   :cond_0
   invoke-virtual {p0}, Lcom/app/library/core/CoreActivity;->getWindow()Landroid/view/Window;

   move-result-object v0

   invoke-virtual {v0, v1, v1}, Landroid/view/Window;->setFlags(II)V

   .line 47
   :cond_1
   return-void
.end method
```

Patching meth: bool var overwrite

app/smali/com/acme/library/core/CoreActivity.smali

```
.method protected onCreate(Landroid/os/Bundle;)V
   […SNIP…]

   iget-boolean v0, v0, Lcom/app/library/core/config/CoreConfig;->allowScreenshots:Z

   const/4 v0, 0x1 #successful patch

   if-nez v0, :cond_1

   .line 44
   :cond_0
   invoke-virtual {p0}, Lcom/app/library/core/CoreActivity;->getWindow()Landroid/view/Window;

   move-result-object v0

   invoke-virtual {v0, v1, v1}, Landroid/view/Window;->setFlags(II)V

   .line 47
   :cond_1
   return-void
.end method
```

Patching meth: force skipping

app/smali/com/acme/library/core/CoreActivity.smali

```
.method protected onCreate(Landroid/os/Bundle;)V
   […SNIP…]

   iget-boolean v0, v0, Lcom/app/library/core/config/CoreConfig;->allowScreenshots:Z

   :cond_1 #force skipping to :cond_1 (successful patch)

   if-nez v0, :cond_1

   .line 44
   :cond_0
   invoke-virtual {p0}, Lcom/app/library/core/CoreActivity;->getWindow()Landroid/view/Window;

   move-result-object v0

   invoke-virtual {v0, v1, v1}, Landroid/view/Window;->setFlags(II)V

   .line 47
   :cond_1
   return-void
.end method
```

Terminology Confusion

- Dalvik & ART

Challenges

- Obf
- CRC

Conclusion

Qs?

- @pagvac @MinervaSec

Resources

- https://androidcracking.blogspot.com/
- http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html
- https://pen-testing.sans.org/blog/2015/06/30/modifying-android-apps-a-sec575-hands-on-exercise-part-1