

## <실습 3>

---

**Youn Kyu Lee**  
Hongik University

# 실습 3

---

**3-1 애플리케이션 패칭**

**3-2 안드로이드 키보드 캐시 이슈**

# 실습 3

---

## 3-1 애플리케이션 패칭

## 3-2 안드로이드 키보드 캐시 이슈

# 애플리케이션 패칭

## 취약점

- 안드로이드 코드를 변경하여 비정상적인 동작을 수행하도록 APK 변조할 수 있다.
- 변조된 애플리케이션은 개인 정보, 민감 정보 탈취, 인증 무력화 등의 동작을 수행한다.



# 애플리케이션 패칭 (1)

## 1. 기존 apk 삭제 및 apktool 설치

(1) smali나 resource 파일들을 수정하고 새로운 apk를 AVD에 설치하기 전에 AVD에서 같은 이름을 갖는 기존 apk를 삭제해야 한다.

(2) 삭제할 앱 (InsecureBankv2) 의 이름을 찾기 위해서 아래의 명령어들을 PowerShell 상에서 차례대로 실행한다.

PS> adb root

PS> adb shell

(3) adb 프롬프트상에서 다음의 명령어를 수행한다.

# ls /data/data | grep insecure

```
generic_x86:/ # ls /data/data | grep insecure
com.android.insecurebankv2
```

- 출력되는 앱의 이름이 com.android.insecurebankv2 인 것을 확인한다.

# 애플리케이션 패칭 (2)

---

(4) 다음의 명령어를 adb 프롬프트상에서 실행하여 해당 앱을 삭제한다.

```
# pm uninstall com.android.insecurebankv2
```

(5) 아래 경로에서 Apktool (apktool.jar 파일과 apktool.bat 파일)을 다운받은 뒤, C:\Windows에 위치시킨다.

- <https://ibotpeaches.github.io/Apktool/install/>

# 애플리케이션 패칭 (3)

## 2. AndroLabServer 구동

(1) PowerShell 구동 후, 아래의 명령어 입력하여 경로를 변경한다.

```
PS> cd ~\Desktop\InsecureBankv2\AndroLabServer
```

(2) 아래의 명령어를 입력하여 AndroLabServer 구동한다.

```
PS> python .\app.py
```

(3) 정상적으로 구동 시, 아래의 메시지가 출력된다.

```
(netsec) PS C:\Users\> cd ~\Desktop\InsecureBankv2\AndroLabServer
(netsec) PS C:\Users\> Desktop\InsecureBankv2\AndroLabServer> python .\app.py
The server is hosted on port: 8888
```

# 애플리케이션 패칭 (4)

## 3. InsecureBankv2 앱 패칭

(1) 안드로이드 스튜디오에서 InsecureBankv2 프로젝트를 열고 나서  
Build -> Build APK를 선택한다.

(2) PowerShell상에서 다음의 명령어를 실행한다.

```
PS> cd
```

```
~\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug
```

```
PS> apktool d app-debug.apk
```




# 애플리케이션 패칭 (5)

(3) app-debug 폴더 생성 여부를 확인한 후, 아래 경로로 이동한다.

~\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug\app-debug\smali\com\android\insecurebankv2

(4) PostLogin.smali 파일에서 “Device not Rooted” 문자열을 본인 이름 문자열(예. “Youn Kyu Lee”)로 변경한 후 저장한다.

<pre>root_status:Landroid/widget/TextView;  const-string v2, "Device not Rooted!!"  invoke-virtual {v1, v2}, Landroid/widget,</pre>		<pre>iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;-&gt;root_status:Landroid/widget/TextView;  const-string v2, "Youn Kyu Lee!!"  invoke-virtual {v1, v2}, Landroid/widget/TextView;-&gt;setText(Ljava/lang/CharSequence;)V</pre>
---	--	---

# 애플리케이션 패칭 (6)

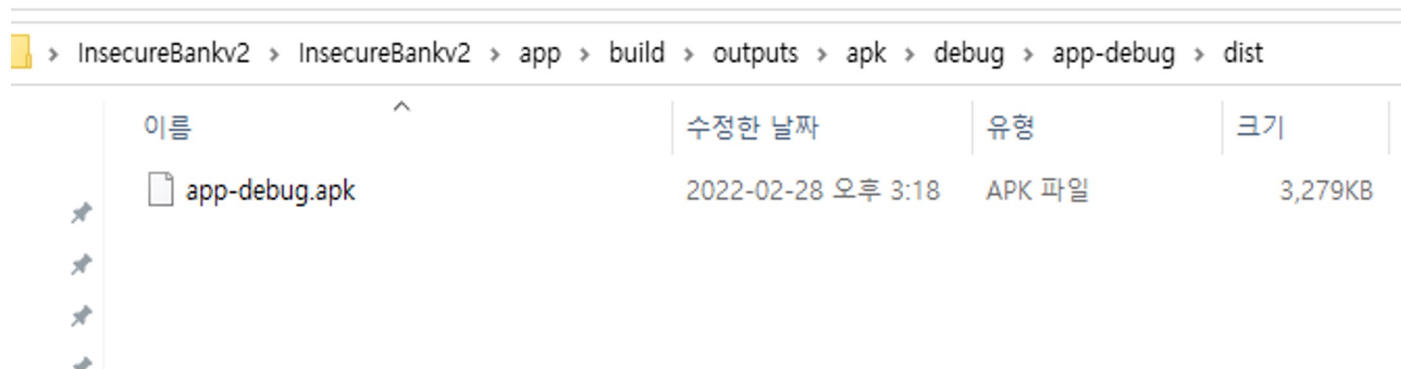
(5) PowerShell상에서 다음의 명령어를 실행한다.

```
PS> cd
```

```
~\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug
```

```
PS> apktool b app-debug
```

- ~\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug\app-debug\dist 폴더안에 변경된 내용을 포함하는 app-debug.apk가 생성된다.

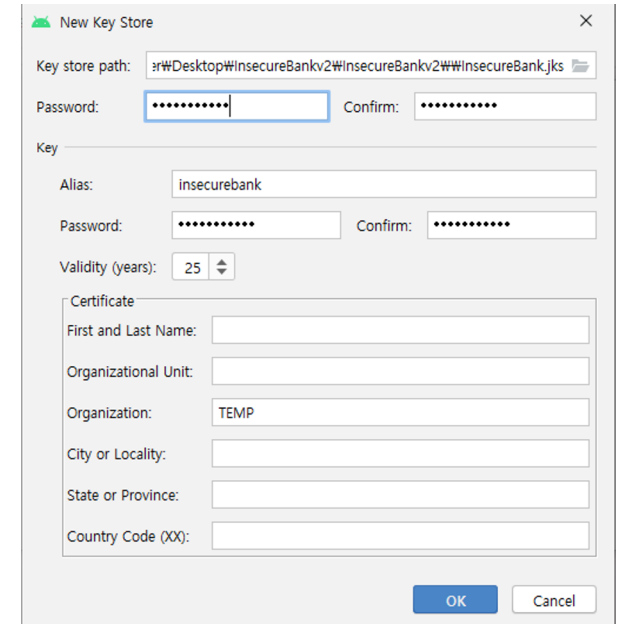


이름				수정한 날짜	유형	크기
app-debug.apk				2022-02-28 오후 3:18	APK 파일	3,279KB

# 애플리케이션 패칭 (7)

(6) 안드로이드 스튜디오 실행 -> InsecureBankv2 프로젝트를 오픈 -> Build -> Generate Signed Bundle or APK -> APK를 선택 -> Next를 선택 -> Create new 버튼을 눌러서 다음과 같이 설정한다.

- KeyStore path: C:\Users\컴퓨터의 사용자 이름\Desktop\InsecureBankv2\InsecureBankv2\insecurebank.jks
- password: insecure123
- Key alias: insecurebank
- KeyStore password: insecure123
- Certificate의 Organization: TEMP



New Key Store

Key store path: r:\Desktop\InsecureBankv2\InsecureBankv2\InsecureBank.jks

Password: insecure123 Confirm: insecure123

Key

Alias: insecurebank

Password: insecure123 Confirm: insecure123

Validity (years): 25

Certificate

First and Last Name:

Organizational Unit:

Organization: TEMP

City or Locality:

State or Province:

Country Code (XX):

OK Cancel

설정을 완료한 후 OK를 선택해 Key Store를 생성하고, Generate Signed Bundle or APK 창에서는 Cancel을 선택해 빠져나온다.

# 애플리케이션 패칭 (8)

(7) PowerShell 상에서 아래의 폴더로 이동한 후,  
~\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug

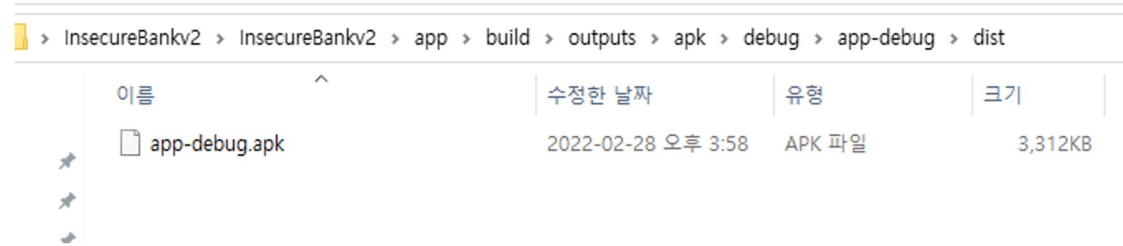
다음의 서명 작업을 수행한다.

```
PS > jarsigner.exe -verbose -sigalg MD5withRSA -digestalg SHA1 -keystore  
C:\Users\컴퓨터의 사용자 이름  
\Desktop\InsecureBankv2\InsecureBankv2\insecurebank.jks C:\Users\컴퓨터의 사  
용자 이름  
\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug\app-  
debug\dist\app-debug.apk insecurebank
```

- 위의 서명 작업 중에서 마지막의 insecurebank는 Key alias 값이다.
- 명령어 입력 후, password(insecure123)를 입력한다.

# 애플리케이션 패칭 (9)

(8) 다음의 폴더에 새롭게 서명된 app-debug.apk 파일 존재 여부를 확인한다.  
~\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug\app-debug\dist\ 폴더에 새롭게 서명된 app-debug.apk 파일이 존재하는 것을 확인한다.

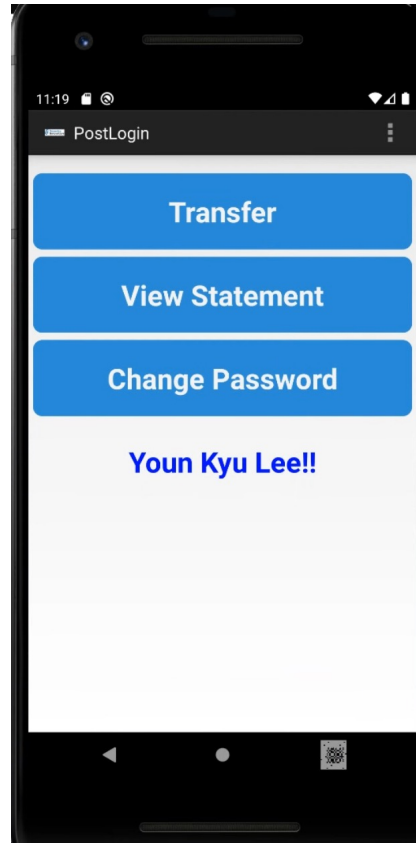


(9) 안드로이드 스튜디오를 실행시킨 후, 안드로이드 가상 디바이스 (AVD)를 띄운다. PowerShell상에서 다음의 경로로 이동한 후,  
~\Desktop\InsecureBankv2\InsecureBankv2\app\build\outputs\apk\debug\app-debug\dist\  
아래 명령어를 실행하여 새롭게 서명된 InsecureBankv2 앱을 AVD에 설치한다.

PS > adb install app-debug.apk

# 애플리케이션 패칭 (10)

(10) InsecureBankv2 앱을 설치한 후 InsecureBankv2 앱에 로그인 (아이디:dinesh, 패스워드: Dinesh@123\$)한 후에 화면에 나오는 메시지가 본인 이름 문자열로 변경되었는지 확인한다.



# 실습 3

---

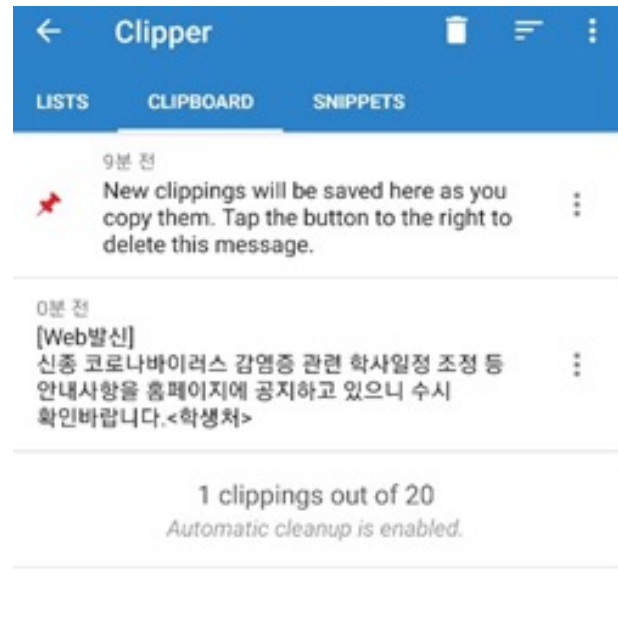
3-1 애플리케이션 패칭

**3-2 안드로이드 키보드 캐시 이슈**

# 안드로이드 키보드 캐시 이슈

## 취약점

- 사용자가 정보를 클립보드에 복사하면, 해당 데이터는 키보드 캐시에 임의로 저장된다.
- 해당 내용이 필요한 경우, 캐시에 저장된 정보를 불러와서 입력한다.
- 사용자가 클립보드에 저장한 정보는 제 3자가 열람하여, 악의적으로 사용될 수 있다.





# 안드로이드 키보드 캐시 이슈 (1)

## 1. AndroLabServer 구동

(1) PowerShell 구동 후, 아래의 명령어 입력하여 경로를 변경한다.

```
PS> cd ~\Desktop\InsecureBankv2\AndroLabServer
```

(2) 아래의 명령어를 입력하여 AndroLabServer 구동한다.

```
PS> python .\app.py
```

(3) 정상적으로 구동 시, 아래의 메시지가 출력된다.

```
(netsec) PS C:\Users\# > cd ~\Desktop\InsecureBankv2\AndroLabServer
(netsec) PS C:\Users\# \Desktop\InsecureBankv2\AndroLabServer> python .\app.py
The server is hosted on port: 8888
```

# 안드로이드 키보드 캐시 이슈 (2)

---

## 2. InsecureBankv2 앱 구동

(1) AVD 상에 InsecureBankv2 앱을 빌드 및 설치 후 구동한다.

(2) secureBankv2 앱에 대한 로그인을 완료한다.

- id: dinesh
- pwd: Dinesh@123\$

# 안드로이드 키보드 캐시 이슈 (3)

## 3. 안드로이드 키보드 캐시 이슈

(1) 아래 경로에서 Clipper\_Clipboard\_Manager\_v2.4.17\_apkpure.com.apk을 다운받은 후, 해당 파일의 이름을

Clipper\_Clipboard\_Manager\_v2.4.17\_apkpure.com.apk로 변경한다.

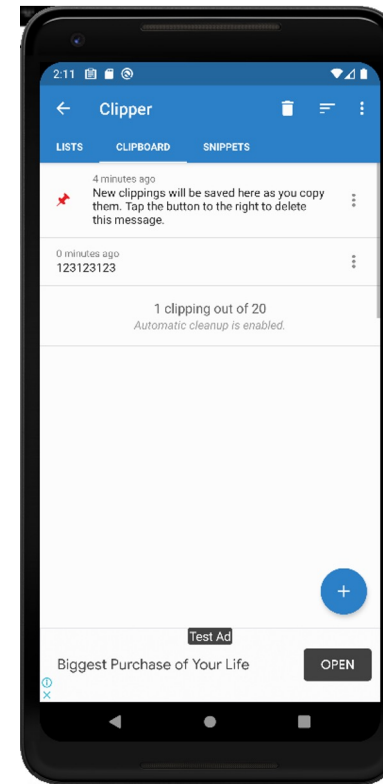
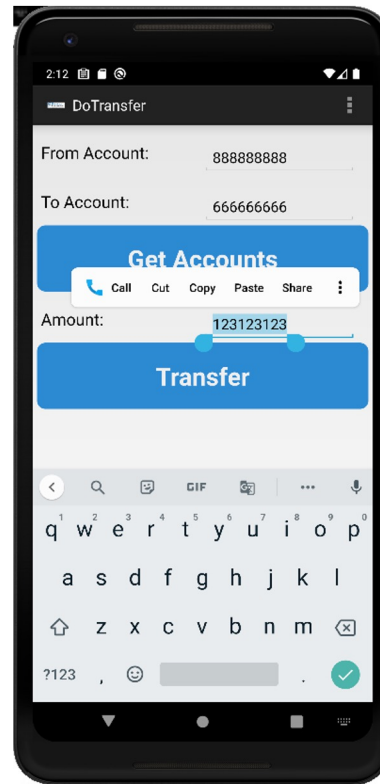
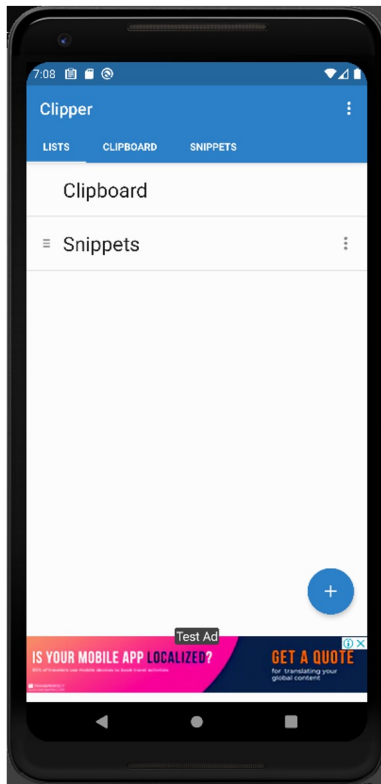
\*경로: <https://apkpure.com/kr/clipper-clipboard-manager/org.rojekti.clipper>

(2) PowerShell 상에서 다운받은 위치로 이동 후 다음의 앱 설치 명령어를 수행하여, Clipper\_Clipboard\_Manager\_v2.4.17\_apkpure.com.apk 앱을 AVD에 설치한다.

PS> adb install Clipper\_Clipboard\_Manager\_v2.4.17\_apkpure.com.apk

# 안드로이드 키보드 캐시 이슈 (4)

(3) 설치한 clipper를 실행한 후에, InsecureBankv2 앱에서 이체 금액이나 계좌번호를 복사한 후, Clipper를 확인한다.



- Clipper를 확인하면, 복사했던 정보가 저장되어 있는 것을 확인할 수 있다.

---

# Q & A

[aiclasshongik@gmail.com](mailto:aiclasshongik@gmail.com)

---