NFSU National Forensic Sciences University
Knowledge | Wisdom | Fulfilment

An Institute of National Importance
(Ministry of Home Affairs, Government of India)

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in

Access Control Issues:

Access Control Issues - I

Calling Activity using Intent

Access Control Issues - I

- ✓ Android has a very complex architecture. It has built on Linux kernel, Dalvik Virtual Machine and much more. but it has four vital components.
    - ✓ **Activities:** An activity is a single, focused thing that user can interact with.
    - ✓ **Content Provider:** Manages access to a central repository of data provided by an application.
    - ✓ **Broadcast Receiver:** Android apps broadcast messages to each other. The broadcast receiver process called Broadcast Receiver.
    - ✓ **Services:** Background processes to handle long term jobs.

Access Control Issues - I

- Components of applications should not be accessed by other applications.
- In some cases an android application shares its resources with other applications.
- For example, we can make call by sending an intent. To give such an access:
    - The host application should declare a permission.
    - The shared component should not disclose any secret data.
    - The component should not threaten the user privacy.

Access Control Issues - I

- ✓ Next three tasks in the DIVA application will show the threats of insecure access to the components.
- ✓ We will exploit this vulnerability, manually and using Drozer also.

Access Control Issues - I

- ✓ a. Access control issues arises when application does not authenticate user.
- ✓ b. Authorization chedk is mission
- ✓ c. Attacker with un-sufficient privilege can see the protected resource.
- ✓ This may be the case when attacker tries to access any sensitive information without authentication or if he / she authenticated but not authorized.

Access Control Issues - I

- ✓ It means that if developer does not manage authentication or authorization to access any resource this vulnerability may exist and can results in loss of sensitive information disclosure.

Access Control Issues – I (Practical)

- ✓ f.Challenges is available with options view API credential, means when you click on this button it opens one activity though which you can access / see API credential.
- ✓ g.Our job is to access this API credential directly through the activity without clicking on that button.
- ✓ h.Just open the DIVA and check what happen when you click on Access Control Issues – Part. As you can finds that after clicking the button it opens one activity which shows API key, Username and Password.

Access Control Issues – I (Practical)

- ✓ i. Now challenges is to show same sensitive information that is API key, Username and Password without clicking the button or without opening the DIVA application also.

Access Control Issues – I (Practical)

- ✓ j.Let’s open the source code and understand it.
- ✓ k.Decompile the APK file with jadx
- ✓ l.santoku@santoku:-$ cd desktop
- ✓ m.santoku@santoku:Desktop:# cd jadx/
- ✓ n.santoku@santoku:Desktop/ jadx/: #cd bin
- ✓ o.santoku@santoku:Desktop/jadx/bin/:#cd diva/
- ✓ p.santoku@santoku:Desktop/jadx/bin/diva:#ls
- ✓ q.find android, AndroidManifest.xml, jakhar, and res files and directories

Access Control Issues – I (Practical)

- ✓ r.santoku@santoku:Desktop/jadx/bin/: # vim AdndroidManifest.xml
- ✓ s.you can finds all the activity with their respective permission in the manifest file.
- ✓ Find the activity entry android name=”jakhar.aseem.diva.AccessControl1Activity”, this activity which contain button label with ViewAPICredentials and when we click on it as we observed it will open one more activity which is registered as android

Access Control Issues – I (Practical)

- ✓ t.name=”jakhar.aseem.diva.APICredsActivity” in the manifest.xml file. This activity contain sensitive information related to API.
- ✓ u.Now AccessControl1Activity invokes the APICredsActivity activity using <intent-filter> activity
- ✓ <action android name=”jakhar.aseem.diva.action.VIEW_CREDS” which contain API sensitive data.

Access Control Issues – I (Practical)

- ✓ v.Now copy the above filter intent and opens using activity manger directly
- ✓ w.Every android has activity manger and we will use same.
- ✓ x.santoku@santoku:/$ adb shell
- ✓ y.root@santoku:/am // and you can see all the help / information related to activity mangar.

Access Control Issues – I (Practical)

- ✓ z.root@santoku:$: am start –a jakhar.aseem.diva.action.VIEW_CREDS // intent filter
- ✓ aa.hit enter and see in the Genymotion that the said activity has opened without clicking the button and it shows same sensitive information.

NFSU National Forensic Sciences University
Knowledge | Wisdom | Fulfilment

An Institute of National Importance
(Ministry of Home Affairs, Government of India)

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in