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

External Insecure Data Storage (SD Card)

Do not store sensitive information on external storage (SD card) unless encrypted first

External Insecure Data Storage

- ✓ Android provides several options to save persistent application data, one of which is External Storage (/sdcard, /mnt/sdcard). "External storage"
- ✓ examples include a micro- or standard-sized SD card internal to the device, Android device storage mounted to a PC, and the Android/obb directory.
- ✓ Files saved to the external storage prior to Android 4.1 are world-readable. Prior to Android 1, files saved to external storage are world-writable.

External Insecure Data Storage

- ✓ From Android 1 to Android 4.3, only the WRITE_EXTERNAL_STORAGE permission is required for an app to write to any external storage file stored by any app.
- ✓ Starting with Android 4.4, groups and modes of files are created based on a directory structure, which allows an app permission to manage/read/write files within a directory structure based on its package name.

External Insecure Data Storage

- ✓ Starting with Android 4.4, users (including apps as users) are isolated from primary external storage spaces of other apps controlled by the Android device.
- ✓ Consequent to the lack of restrictions described above, files written to external storage can be modified or read by other apps installed on the device (for the Android versions which allow read/write) and by anyone with access to the files if stored on an off-device external storage device such as a PC (or if the in-device external storage media is removed and mounted elsewhere).

External Insecure Data Storage

- ✓ Developers should not store sensitive data to external storage devices unless encrypted first, because files stored externally have no guarantee of availability, integrity, and confidentiality.

External Insecure Data Storage – SD Card

- a.Sometimes android developers stores sensitive information without encryption.
- b.Application might stores dta in external storage (SD card)
  - i./dara/data/[package name]/shared_preferences
  - ii.Databases
  - iii.Temporary files
  - iv.External Storage

- ✓ b.Click Insecure Data Storage – Part 4 and read the objective
- ✓ c.Open the InsecureDataStorage4Activity.class, now do the analysis of the code and found that data is stored in the database
- ✓ a.If check the source code we found that
- ✓ b.File localFile1 = Environment.getExternalStorageDirectory(); shows that localFile1 object is created and reference of external stored is stored with it.

External Insecure Data Storage – SD Card

- ✓ c.If we go ahead we found that
- ✓ d.File localFile2 = new File(localFile1.getAbsolutPath() + “/.uinfo.txt”);
- ✓ e.Which means that uinfo.txt file is created inside the external storage and may contain important information.
- ✓ f.Lets try to find it in the jakhar.aseem.diva directory if we can find it

External Insecure Data Storage – SD Card

- ✓ g.santoku@santoku:-$ adb shell
- ✓ h.root@santoku:/ # cd /data/data/
- ✓ i.root@santoku:/data/data # cd jakhar.aseem.diva/
- ✓ j.root@santoku:/data/data/jakhar.aseem.diva/ # ls –la
- ✓ k.There is no file is available.
- ✓ l.root@santoku:/ cd /mnt/sdcard/
- ✓ m.root@santoku/cd /mnt/sdcard/ : #ls // but you do not finds that file

External Insecure Data Storage – SD Card

- ✓ n.if you check the source code it shows that “./uinfo” where “./” shows that it is hidden file.
- ✓ o.root@santoku/cd /mnt/sdcard/ : # ls –a
- ✓ p.now we can find /uinfo.txt
- ✓ q.root@santoku/cd /mnt/sdcard/ : # cat ./uinfo.txt
- ✓ r.now you can see the username and password

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