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

Insecure Logging

or

Do not log sensitive information

Insecure Logging

- ✓ Android provides capabilities for an app to output logging information and obtain log output.
- ✓ Applications can send information to log output using the android.util.Log class.
- ✓ To obtain log output, applications can execute the logcat command.

Ref:
https://wiki.sei.cmu.edu/confluence/display/android/DRD04J.+Do+not+log+sensitive+information

Insecure Logging

- ✓ To log output
- ✓ The android.util.Log class allows a number of possibilities:

Log.d (Debug)	Log.e (Error)	
Log.i (Info)	Log.v (Verbose)	Log.w (Warn)

- ✓ Log.v("method", Login.TAG + ", account=" + str1);
- ✓ Log.v("method", Login.TAG + ", password=" + str2);
- ✓ To obtain log output
- ✓ Declare READ_LOGS permission in the manifest file so that an app can read log output:

Insecure Logging

- ✓ AndroidManifest.xml:
- ✓ <uses-permission android:name="android.permission.READ_LOGS"/>
- ✓ Prior to Android 4.0, any application with READ_LOGS permission could obtain all the other applications' log output. After Android 4.1, the specification of READ_LOGS permission has been changed. Even applications with READ_LOGS permission cannot obtain log output from other applications.

Insecure Logging

- ✓ However, by connecting an Android device to a PC, log output from other applications can be obtained.
- ✓ Therefore, it is important that applications do not send sensitive information to log output.

Insecure Logging - Applicability

- ✓ Applications should make sure that they do not send sensitive information to log output.
- ✓ If the app includes a third party library, the developer should make sure that the library does not send sensitive information to log output.
- ✓ One common solution is for an application to declare and use a custom log class, so that log output is automatically turned on/off based on Debug/Release.

Insecure Logging - Applicability

- ✓ Developers can use ProGuard to delete specific method calls. This assumes that the method contains no side effects.

Insecure Logging - Related Vulnerabilities

- ✓ Facebook SDK for Android: http://readwrite.com/2012/04/10/what-developers-and-users-can#awesm=~o9iqZAMlUPshPu
- ✓ JVN#23328321 Puella Magi Madoka Magica iP for Android vulnerable to information disclosure
- ✓ JVN#86040029 Weathernews Touch for Android stores location information in the system log file
- ✓ JVN#33159152 Loctouch for Android information management vulnerability
- ✓ JVN#56923652 Monaca Debugger for Android information management vulnerability

Insecure Logging - Risk Assessment

- ✓ Logging sensitive information can leak sensitive information to malicious apps.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
DRD04-J	Medium	Probable	Medium	P8	L2

Insecure Logging –DIVA (Practical)

- ✓ c.Let start DIVA and click on 1. Insecure Logging and enter the value. It shows the error message “An error occurred. Please try again later”. Let do the analysis of the code,
- ✓ d.santoku@santaku:~/ Desktop$ unzip –d diva diva-beta.apk
- ✓ e.santoku@santaku:~/ Desktop$ cd diva/
- ✓ f.santoku@santaku:~/ Desktop$ d2j –dex-jar classes.dex
- ✓ g.santoku@santaku:~/ Desktop$ ls
- ✓ h.santoku@santaku:~/ Desktop$ jd-Igui classes-dex2jar.jar
- ✓ i.check the LogActivity

- ✓ catch (RuntimeExceptionlocalRuntimeException)

{ Log.e(“diva-log”, “Error while processing transaction with credit card:” + localEditText.getText().tostring());

Toast.makeText(this, “An error occurred. Please try again leter”,0).show();

}

- ✓ j.Now find the process id for same and using same process id we can search for entry from the log.
- ✓ k.santoku@santaku:~/ adb shell ps | grep “diva”
- ✓ l.check the second column which shows the process id.

Insecure Logging –DIVA

- ✓ m.santoku@santaku:~/ adb shell logcat | grep “1065”
- ✓ n.now move in the theGenymotion and enter the credit card number and click on check out
- ✓ o.move into the logcat window and check the last entry in the logcat it show the credit card number also. Instead of credit card it may be username password or authentication token.
- ✓ p.One more way to represent the logcat entry is using pidcat
- ✓ q.santoku@santoku: cd pidcat/
- ✓ r.santoku@santoku/pidcat:$ python pidcat.py

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