**Don’t trust that “Encrypted” Android app on Play Store**

Google’s Play Store consists of many apps that market themselves as secure apps, but the fact is that most of them have poorly implemented encryption just for the sake of getting the “secure app” label.

The claim was made by two researchers from the University of Strathclyde, James Irvine and Greig Paul who tested Android app security in detail. The duo selected nine famous apps for their research – some of them developed by “Top Developers” endorsed by Google – and tested them against their claim of protecting photos, videos and passwords through encryption. Surprisingly, these ad-funded apps were unable to prove that the applied encryption tools were catering to the required android app security standard.

All the nine apps under study came out with major security vulnerabilities. While some apps did not even bother encrypting files at all, others encrypted them through a static key which remained the same wherever the app is implemented. This could allow any hacker with basic cracking skills to unlock the key and decipher the information.

The static key of an app Video Locker by Handy Apps was easily recovered by the researchers using “known plaintext attack”. A PIN code used along with the static key was also easily discoverable. Another app called Password Locker by the same app developers had similar vulnerabilities. This app poses even more serious threat because not only does it put passwords at risk but also gives the user an option to synchronize with Google or Dropbox account. Another app, Video Locker Advanced that claims to deploy techniques of fast encryption does not actually use any such techniques and only flips first hundred bits of the file. Also, it was noted that all the nine apps were not open source, which should not be the case especially for security related apps.

Google does not seem to be much interested in improving Android app security as it has not taken any action against misleading app developers. It needs to take strict measures against any misrepresentation of apps and raise the criteria for “top developer” status, particularly for security apps.