**Android lags behind Apple in Security: claims Cryptography Professor**

Matthew Green, a cryptography professor at John Hopkins University has claimed that Android is far behind Apple in terms of security. Android uses full-disk encryption which is the same solution as that of personal computers, which is why it is vulnerable as unlike personal computers, smartphone is never shut down on regular basis. Hence, the cryptographic keys keep lying in the RAM at most times. Apple, on the other hand, encrypts every fill separately by using file based encryption.

“Since phone batteries live for a day or more (a long time compared to laptops) encryption doesn’t really offer much to protect you against an attacker who gets their hands on your phone during this time,” says Green.

Apple’s approach for iOS security provides better protection than android app security, with the introduction of “data protection” feature after the release of iOS 4. The file based encryption was made possible after the provision of an API to developers by which they can state a particular key class to be used while encrypting a file.

iOS comes with different classes for protection; like no protection, protected until first user authentication, and complete protection. For applications there is a fourth class for protection of apps that have to make encrypted files when a class key is removed from the RAM.

Google has planned to improve android app security with the release of Android 7.0 Nougat, which is yet to be released. This new version will introduce two protection classes i.e. device encrypted storage and credential encrypted storage. These are based on a new system called the Direct Boot which can allow android device to get access to some data before a user enters a passcode.

According to Matthew Green, Google does not lag behind in cryptography, but rather Android app security can be improved if Google gives correct guidance to developers, which it is currently lacking.