**Why exactly is Android security so tricky**

Android authentication, though helps identify users, can also be tricky as it can allow access to hackers at the same time. All of this depends upon the device administrator access which, if granted to a hacker, can provide multiple benefits.

Gaining device administrator access means getting complete access to the device which includes being able to create and manage policies, configurations, applications, and even getting API access to the Android device. Since majority of applications in the Play store do not require this level of access to the device, Android app security is put to real test when an application actually does so. In this case, the user has to be aware enough to discontinue the installation. Recent malware exploits have successfully been using this strategy to gain device administrator access to Android devices, and this is why Android app security is tricky especially when a user is not educated enough to understand the risks.

This threat can become more risky if the target is a Bring Your Own Device (BYOD) brought by the user at job, as it not only leaks out the user’s personal information but also corporate data. If employees are using a BYOD for personal as well as corporate use, they need to be provided with an Enterprise Mobility Management (EMM) or Mobile Device Management (MDM) solution that protects corporate information by differentiating clearly between personal and corporate data.

Because device authentication naturally assumes that the person having the device is actually a human, it is hard to effectively authenticate a real user. Behavioral biometrics allows application developers to strengthen Android app security by understanding if they are dealing with real humans or automated response imitating as a human. This in turn allows for another level of device authentication without having the user to experience frustration otherwise felt with simple device authentication.