Prof. Manoj Gaur
MNIT Jaipur
Abstract of talk

"Security Challenges in Android Platform"

Android Smartphone OS is gaining big market share due to its open source nature and rich Application Programming Interface (API). Users and developers are adopting Android due to its open and cost effective appstore model in comparison to other mobile platforms like iOS. At the core of Android is a modified Linux kernel specifically tuned for low-powered, low-memory devices. Register based Dalvik Virtual Machine (DVM) executes dalvik bytecode (dex) efficiently unlike stack based JVM. Android provides security by sandboxing apps at kernel level and permission based model at framework level. Recent versions support tighter security through Security Enhanced Linux to prevent rooting attacks. Android app consists of several components such as Activities, Services, Broadcast Receivers and Content Providers. Binder IPC driver facilitates communication among these components across apps, which is prone to various spoofing and hijacking attacks. Users must accept all the permissions to install an app. Often, inability to judge the implication of those permissions may compromise user security.

Increasing number of Android devices has attracted attention of malware authors who till now concentrated more on Microsoft Windows. Millions of Smartphone users are affected through rooting attacks, premium rate SMS malware, botnets, trojans, spyware. Availability of reverse engineering tools and sophisticated code transformations aid malware authors to bypass anti malware solutions employing traditional signature based methods.

The realization has led to implementing behavior based, profile based, smart signature based methods and dynamic analysis approaches. Conventional desktop PC anti malware solutions may not be replicated on smartphone due to their resource limitations. Alternative approaches including machine learning can be deployed for effective malware detection.

In this talk, we will be covering details of Android OS and emerging security issues with this popular software.
