

ANALYSIS OF ANDROID VULNERABILITIES AND MODERN EXPLOITATION TECHNIQUES

Himanshu Shewale¹, Sameer Patil², Vaibhav Deshmukh³ and Pragya Singh⁴

MS (Cyber Laws and Information Security) Division, Indian Institute of Information Technology, Allahabad, India
E-mail: ¹ims2012014@iiita.ac.in, ²ims2012012@iiita.ac.in, ³ims2012047@iiita.ac.in, ⁴pragyabhardwaj@iiita.ac.in

Abstract

Android is an operating system based on the Linux kernel. It is the most widely used and popular operating system among Smartphones and portable devices. Its programmable and open nature attracts attackers to take undue advantage. Android platform allows developers to freely access and modify source code. But at the same time it increases the security issue. A user is likely to download and install malicious applications written by software hackers. This paper focuses on understanding and analyzing the vulnerabilities present in android platform. In this paper firstly we study the android architecture; analyze the existing threats and security weaknesses. Then we identify various exploit mitigation techniques to mitigate known vulnerabilities. A detailed analysis will help us to identify the existing loopholes and it will give strategic direction to make android operating system more secure.

Keywords:

Android, Vulnerability, Exploit, Malware, Linux Kernel

1. INTRODUCTION

Android is a fast growing and largest installed base of mobile platform which powers millions of mobile devices. Based on the Linux kernel, android operating system is open and flexible enough to run on different mobile devices having varied hardware configuration [6]. This increases the popularity and acceptance of android amongst the users.

Android platform provides developers huge opportunity to develop applications to cater to the needs of its ever increasing user base. The Android platform includes applications, middleware and the operating system [7]. Developers use the AndroidSDK, which consist of various tools and APIs to develop applications using programming language like Java. Android provides an open marketplace wherein developers can sell and distribute applications instantly.

While the openness of android provides a favorable atmosphere for users as well as developers, it also attracts attackers and hackers to take undue advantage [1]. The capability of android to run on different devices and with different versions exposes it to varied security issues. Not all devices can be updated to latest version because of the customization done by different device manufacturer. This result in leaving the old users stay unprotected from latest security issues addressed in the new version [2].

The android marketplace lacks rigorous inspection of the applications being sold and distributed by developers [1]. Applications can be published in the marketplace without any third party's review. It leaves a device running android susceptible to stealing of data that is of corporate or personal use. Smartphones store information like location history, contacts, mails, call register, photos, messages or any other file that is important [2]. Malicious applications can gain access to

user's private information stored in the device. A malware can even try to gain root privileges and abuse the normal functioning of the device [3].

2. ANDROID PLATFORM ARCHITECTURE

The Android platform was created by Android Inc. which was later bought by Google and called it the Android Open Source Project. The software can be freely obtained from a central repository and modified in terms of the license. The Android platform is based on the Linux kernel, which is modified to meet special needs of better power management, memory management and runtime environment. Also, as Android is designed to be used on Smartphones and tablets, it has many changes and updates to the Linux kernel in order to support different devices [2]. The additions include subsystem to control memory and processor, libraries to manage file systems designed for memories, process management and device management.

The Android software stack can be subdivided into five layers: the Linux Kernel and lower level tools, System Libraries, the Android Runtime, the Application Framework and Application layer on top of all. Each layer provides different services to the layer just above it.

2.1 LINUX KERNEL

The Linux kernel is the basic layer equivalent to an abstract level between hardware layer and other software layers in the system. The Android OS is built on top of this Linux kernel with some changes in the architecture made by Google [7]. The kernel contains a vast array of device drivers which makes interfacing to peripheral hardware easy. The kernel provides basic system functionality like memory management, process management, security, device management, network group etc. [7].

2.2 LIBRARIES

On top of the Linux kernel is a set of Android's native C/C++ libraries. The libraries are specific for particular hardware. For example, the media framework library guides playback and recording of various pictures, video and audio formats. Some other important core libraries include Surface Manager, SQLite, WebKit and OpenGL.

2.3 ANDROID RUNTIME

Android Runtime includes set of core Java libraries. Application programmers use Java programming language for developing apps. It includes the Dalvik Virtual machine and Core Java libraries.