Android Security Terrorization

Pratik Parmar

C U Shah University, C U Shah Technical Institute of Diploma Studies, Wadhwan City, Gujarat, India

Abstract: ***Now a day's Smartphone's are booming in the market, almost every second person on the earth carries this small computer everyday with them. Smartphone OS like android and iOS are showing us the glimpse of the future. Android has already gained significant advantage in terms of market share because of its features, one of them being the open source OS makes it free and allows persons to customize it, but with such great advantages comes a biggest threat which is security issues. This paper will present the security issues of Android Smartphone's.***

Keywords: Android, Android Security, Threats, Security Terrorization. Smartphone

1. Introduction

Android is a open source OS for Smartphone's which was initially released as Android beta in November 2007 Developed by the Open Handset Alliance (visibly led by Google), based on Linux platform. The first commercial version Android 1.0 was launched in September 2008. Android is the operating system that runs almost one million phones and tablets. Since these devices make our lives sweet each android version is named after a desert.

- Alpha (1.0)
- Beta (1.1)
- Cupcake (1.5)
- Donut (1.6)
- Eclair (2.0–2.1)
- Froyo (2.2–2.2.3)
- Gingerbread (2.3–2.3.7)
- Honeycomb (3.0–3.2.6)
- Ice Cream Sandwich (4.0–4.0.4)
- Jelly Bean (4.1–4.3.1)
- KitKat (4.4–4.4.4, 4.4W–4.4W.2)
- Lollipop (5.0–5.1.1)

Android is a victim of its own success, not just in the way it has attracted malicious attention, but in its very nature. The main advantage of using android is its openness, which in terms puts it at risk of security. This demands the study of the Security terrorization for Android and let the user be aware of how to be careful against such terrorization. The open nature of Android and its large user base have made it an attractive and profitable platform to attack. Common exploits and tool kits on the OS can be utilized across a wide number of devices, meaning that attackers can perform exploits en masse and re-use attack vectors. The paper explains architecture of Android, overview of Android, current state of Android and security terrorization of Android.

2. Architecture of Android

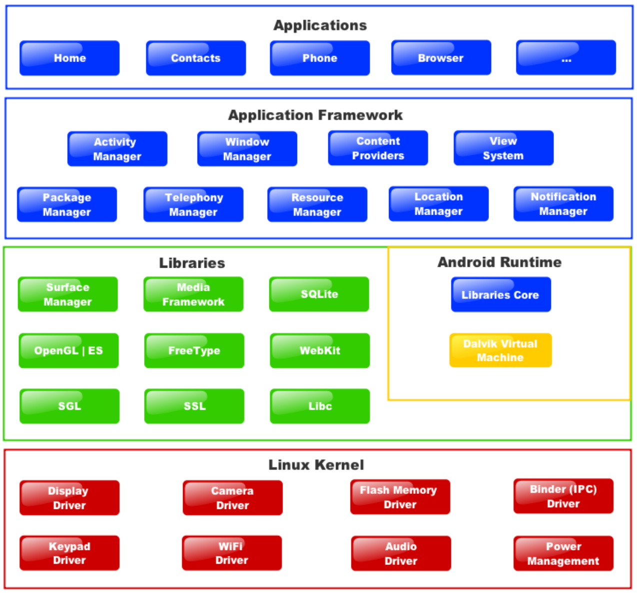

Figure 1: Architecture of Android OS

So, the layers we referred to in the top are:
1. Linux Kernel
2. Libraries & Android Run time
4. Application Framework
5. Android Apps
The app that we develop will go to the Android Apps layer.

2.1. Linux Kernel

Kernel of Android is Linux 2.6 core which, Similar to a desktop computer running Linux, the Android kernel will take care of power and memory management, device drivers, process management, networking, and security. The Android kernel is available at http://android.git.kernel.oro

2.2. Libraries and Android Run-time

This layer is mainly associated with the process running. The core library provides most of the features of Java programming language. Additionally, each program of Android has a separate Dalvik's Java virtual machine environment.

2.3. Application Framework

This layer is developed specifically for allowing developers full access to the core application framework used by the API. It consists of a range of services and system structure which include Active Manager, Windows Manager, View system, Contents Provider, Package Manager, Resource Manage, and so on.

2.4. Applications

The application component of the Android operating system is the closest to the end user. This is where the Contacts, Phone, Messaging, and Angry Birds apps live. As a developer, your finished product will execute in this space by using the API libraries and the Dalvik VM .this includes a core application package, such as Email Client, Web Browser etc.

3. Overview of Android

Android is the operating system that powers more than one million smartphones and tablets. It was designed in November 2007 as Android beta. The first marketable version was released in September 2008. Android is under ongoing development by Google and the Open Handset Alliance (OHA), and has seen a number of updates to its base operating system since its initial release. Since Android is making our lives much sweeter all its released are named after a desert. Given are the versions of android OS and main features of the release.

- **Cupcake (1.5)**
  Bluetooth A2DP
  AVRCP support
  Soft-keyboard with text-prediction
  Record/watch videos
- **Donut (1.6)**
  Gesture framework
  Turn-by-turn navigation
- **Eclair (2.0–2.1)**
  HTML
  Digital zoom
  Microsoft Exchange support
  Bluetooth 2.1
  Live Wallpapers
  Updated UI
- **Froyo (2.2–2.2.3)**
  Speed improvements
  JIT implementation
  USB Tethering
  Applications installation to the expandable memory
  Upload file support in the browser
  Animated GIF
- **Gingerbread (2.3–2.3.7)**
  Updated UI
  Improved keyboard ease of use
  Improved copy/paste
  Improved power management
  Social networking features
  Near Field Communication support
  Native VoIP/SIP support
  Video call support
- **Honeycomb (3.0–3.2.6)**
  Multi core support
  Better tablet support
  Updated 3D UI
  Customizable home screens
  Recent applications viewing
  Redone keyboard layout
  Media/Picture transport protocol
  Google Talk video chat
  Google eBooks
- **Ice Cream Sandwich (4.0–4.0.4)**
  Facial recognition (Face Unlock)
  UI use Hardware acceleration
  Better voice recognition (dictating/Voice typing)
  Web browser, allows up to 16 tabs
  Updated launcher (customizable)
  Android Beam app to exchange data through NFC
- **Jelly Bean (4.1–4.3)**
  Google Now
  Voice Search
  Speed enhancements
  Camera app improvements
- **KitKat (4.4)**
  Screen recording
  New Translucent system UI
  Enhanced notification access
- **Lollipop (5.0)**
  More tangible interaction
  Security
  Power saving
  Customization

4. Current State of Android

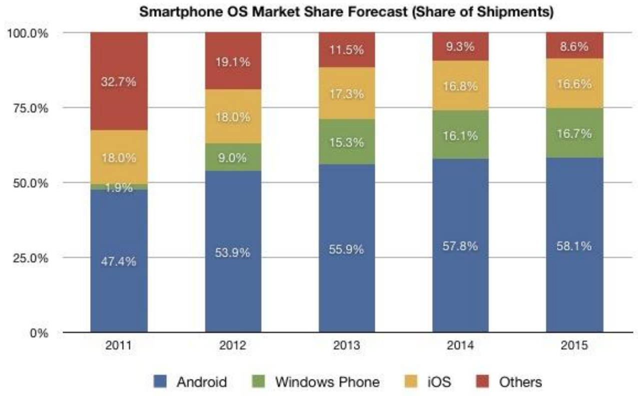

Figure 2: Market share of Android OS in last 5 Years

As the figure 2 suggests the market share of Android OS is increasing every year. Comparing year 2011 with 2015 almost 10% market share increased in Android. Its expected to grow even more. The reason behind it is the openness of android. Android is leading the market with 58.1% market share. Android is the most popular OS amongst any other smartphone OS.

5. Security Threats

Given are the list of threats that may arise in any smartphone with android OS.

5.1. User as admin

Install apps, grant app permissions, download data, and access unprotected networks - The user can reign free over their Android domain without restriction.

5.2. The Android Market

Google's verification processes for applications entering their market have been shown to be woefully lacking over the last year or two, leading to a number of malware-infected apps and games being made legitimately available to users.

5.3. Gateway to PC

Any Android device can be connected to a PC via a USB cable, laying out the contents of its SD card for read/write/ delete. The SD card itself as removable storage can be easily accessed directly as well. Indeed these methods could be utilised themselves for bringing malware in to a corporate network, for downloading malicious content on to a PC or sucking up data as soon as it is connected.

5.4. Application Permissions

In the form of a pop up, the user may see these notifications as a nuisance, a delay in accessing the newly downloaded Angry Birds levels. Or they may simply not understand the nature of the requests. Common permissions that may (read: should!) raise an eyebrow would include 'Read/Send SMS', 'Access Fine Location', 'Access IMEI, phone identity', 'Brick' (required to disable the device in trace and wipe apps), 'Access camera', and so on. Such requests may be integral to functionality, but could equally be recording calls and transmitting sign-in credentials.

5.5. Malicious Application Injections

Data/process transfers between virtualised application environments are handled by a protocol of implicit and explicit intents. Transmission or interception of an intent by a malicious application can result in data being compromised as the target app will respond to the string, potentially resulting in data loss.

5.6. Third Party Applications

One of the great things about Android is choice in terms of standard functionality, such as address books, messaging, keyboards, etc. I'm sure no one in the information security industry would need an explanation as to why it might not be a good idea to use an untrusted third party keyboard or password manager. In a rapidly growing OS environment it can be difficult to identify reputable vendors, and considering the nature of the Android community, can you trust a bedroom programmer with your credentials? Even reputable services can get mobile applications wrong, both Facebook8 and Twitter9 transmit mobile app data in the clear, i.e. without encryption, on nearly all devices. This happens despite the development of such security measures for web app versions.

5.7. Rooting

Rooting an Android device is askin to jail-breaking an iPhone, it opens out additional functionality and services to users. The process of gaining root access, requires the device to be switched from S-On to S-Off (where S = security). Additionally, root is a common exploit used by malicious applications to gain system-level access to your Android. DroidKungFu is one such threat that can root a system and install applications at that level, it escapes detection by utilising encryption and decryption to deliver a payload.

5.8. Wi-Fi

The vulnerability of Android devices running 2.3.3 to compromise on unprotected Wi-Fi networks apparently came as a surprise to many11 – it shouldn't have, when is this practice ever safe?! Beyond highlighting the need for better consumer security awareness, it leads to some other considerations around secure Wi-Fi access. Ideally sign in credentials should always be completed over a secured network, but sometimes this isn't enough. FaceNiff is an easily downloadable application that allows the user to intercept the social networking logins of any Android on their network12. The only way this exploit won't work is if the user is utilising SSL. Furthermore, devices running 2.3 (or rooted older devices) can act as a Wi-Fi hotspot – as an Information Security Manager, how happy would you be about unverified users and devices connecting to a smartphone with a corporate footprint?

5.9. Remote installation

All versions of Android were at one point vulnerable to the remote writing of malicious JavaScript to the SD card through accessing an infected web page13 – an html download does not prompt for user confirmation on the OS, it simply happens. This is now restricted to versions 2.2 and below as the issue was addressed by Google in the Gingerbread (2.3) update. For devices still operating versions with this vulnerability, using Opera Mobile instead of the default web browser will trigger a confirmation when such download attempts begin, allowing the user to deny access.

6. Conclusion

The booming trend of smartphones and its wide adoption to market has increased the chances of security threats. The paper explored the current state of android and its architecture along with the common security threats of Android Os.

References

[1] "Android", at: https://www. android.com/
[2] "AndroidSecurityOverview"at:http://source.android.com/devices/tech/security/index.html

[3] "Mobile Attacks and Defense", Charlie Miller Accuvant Labs, page no .68-70

[4] Sohail Khan, Mohammad Nauman, Abu Talib Othman, Shahrulniza Musa International Conference on, "How Secure is your Smartphone: AnAnalysis of Smartphone Security Mechanisms", International Conference on Cyber Security, Cyber Warfare & Digital Forensic" 2012

[5] "Security in Android Based Smartphone" , Mr. Sumedh P. Ingale, Prof. Sunil R Gupta at www. ijeaim.org

[6] White paper on "A Brief guide to android security" by Ryan Farmer

Author Profile

Pratik Parmar received the B.E. degree in Computer Engineering from C U Shah College of engineering and technology in 2008. During 2008-2015, he has worked in C U Shah Technical Institute of Diploma Studies, Wadhwan City as lecturer in Computer engineering department.