# A need of time: Android Security

Mr. Prashant.V
Student
Information Science
New Horizon College
of Engineering

Mr. Nagendra Devadiga
Student
Information Science
New Horizon College
of Engineering

Mrs.Vandana.C.P
Assistant Professor
Information Science
New Horizon College
of Engineering

**Abstract**-With millions of free applications on the Android Store, users are tempted to download these applications. These apps maybe games or any productive app like Antivirus or Office related apps. Smartphones have become a big essential to everyone’s life. Since user confidential data is accessed by these applications, the user security is at threat. In this paper, the various aspects of security attack in android is analyzed, particularly attacks using cameras.

**Keyword**: Android, Security, Camera based attacks, Spy Cam

## 1.Introduction

Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices.

Android's user interface is based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input.

As of 2015, Android has the largest installed base of all operating system

Android Inc. was founded in Palo Alto of California, U.S. by Andy Rubin, Rich miner, Nick sears and Chris White in 2003. Later Android Inc. was acquired by Google in 2005. [12]

**Android Versions:**

The various Android Versions are shown below[13]

| Code name | Version number | Initial release date |
|---|---|---|
| Cupcake | 1.5 | April 27, 2009 |
| Donut | 1.6 | September 15, 2009 |
| Eclair | 2.0–2.1 | October 26, 2009 |
| Froyo | 2.2–2.2.3 | May 20, 2010 |
| Gingerbread | 2.3–2.3.7 | December 6, 2010 |

| | | |
|---|---|---|
| Honeycomb[a] | 3.0–3.2.6 | February 22, 2011 |
| Ice Cream Sandwich | 4.0–4.0.4 | October 18, 2011 |
| Jelly Bean | 4.1–4.3.1 | July 9, 2012 |
| KitKat | 4.4–4.4.4, 4.4W–4.4W.2 | October 31, 2013 |
| Lollipop | 5.0–5.1.1 | November 12, 2014 |
| Marshmallow | 6.0–6.0.1 | October 5, 2015 |

### 1.1 Security

Security is very essential in an android smartphone. Android is manufactured by google so google asks the user to login to a google account for using any service. Suppose a users' phone is stolen then the thief could access the personal information and his google account.

So smartphone security is very essential. Hackers upload malicious apps on google play store [6] and other third party stores which could steal the users' information. [7]

## 2.Android Platform

### 2.1 Environments of Smartphones

Smartphones can be connected to various devices, PC and other mobile devices using wireless network or cable. This is why smartphones are very popular. This feature allows a malicious attacker or a software to invade smartphones in various paths. The figure 1 shows the environment of smartphone

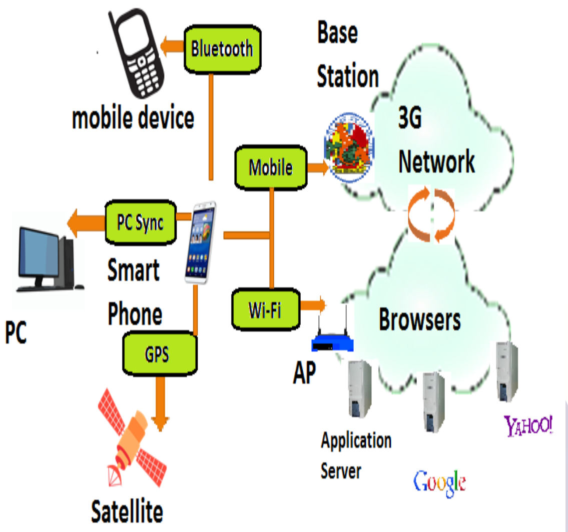

**Fig.1 Environment of smartphone**

The user can make and receive a call, manage his/her schedules, play game or use the other functions of the smart phone. The base station is a way to connect to web and it is also the base for calling service.

A satellite is used to provide location information of smartphones. This is used for map, messenger, and also when a picture is captured using camera, the location name is also inserted in the picture.

A Personal Computer(PC) can be connected to a smartphone using a cable or a wireless network.

### 2.2 Assets of smartphone

**Private information-** Phone book, Call history, Location, Schedule, browsing history/ Cache file, passwords, attachments, and other information

**Device**-Smartphone device, System resources (CPU, RAM, battery etc.)

**Applications-**The apps the user installs.

The information in a smartphone can be defined an asset of smartphone. These data includes the data which are stored in the smartphone's memory as well as the information which is transmitted out of the smartphone.

The phonebook, call history, location, history, Email, SMS etc. are managed by the applications of smartphone.

Smartphone and its resources itself is an asset.

Applications itself is also an asset as some applications are free to use and are uploaded on the Android store and some apps can be bought, thus the application itself is an asset. Some browsers store user id and passwords making the smartphone an asset.

An android smartphone is like a combination of many devices such as MP3 player, Camera, an e-book reader and a GPS device. We can use all this on the go. It would be really tedious if we had to carry all these devices individually. All these features integrated in a smartphone makes it portable.

Smartphones have a touch interface GUI which makes it really easy to use. Google constantly makes sure to improve the GUI and to keep the accessibility as simple as possible to attract all age groups to use the device. Another major advantage of smartphones is that Google keeps updating and fixes the known bugs. Another advantage is that users can use a smartphone like a portable PC. Applications such as Paint, Office, Photo editors, Calories consumed, Reminders, Alarms, check your heart rate and many more productive apps are available.

### 2.3 Android Architecture

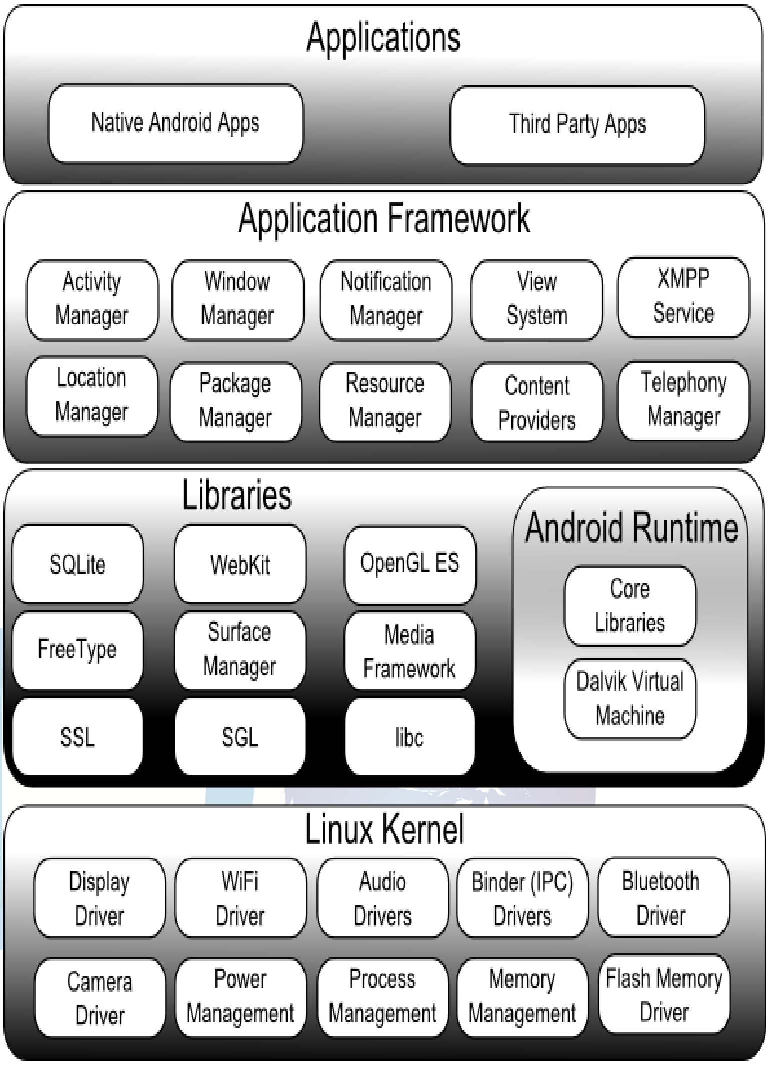

**Fig.2 Android architecture**

Figure 2 shows the Android architecture. Android operating system comprise of different software components arranges in stack. Different components of android operating system are –

1.Linux kernel
2.Libraries
3.Android Run time
4.Application Framework
5.Applications

## 3.Security in Android

### 3.1 Mechanism

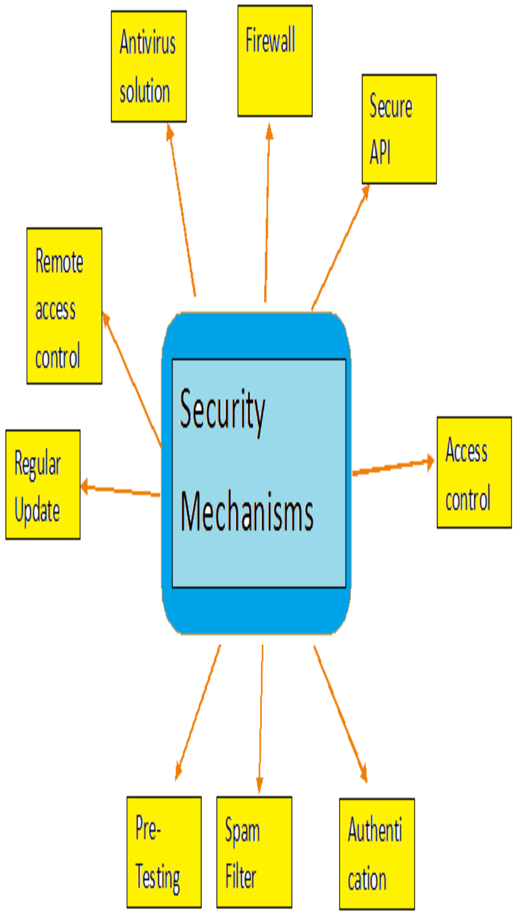

**Fig.3 security mechanisms**

Security is very essential in a phone. The security could be security code, biometric etc. The various security mechanisms as shown in Fig. 3 Android are:

1. **Antivirus**: Antivirus is an application software which is used to scan various files, SMS, MMS, E-Mail and URLs. They detect viruses and prevent attacks. [5][8]
2. **Firewall**: It controls incoming and outgoing network traffic. It denies access to untrusted Wireless networks. [4]
3. **Secure API**: They provide cryptographic functionalities for users and developers.
4. **Access control**: They restrict or block accesses to certain services, processes or apps.
5. **Authentication**: They prevent unauthorized user access. User should be authenticated to use device.
6. **Spam Filter**: Spam filter blocks MMS, SMS, emails and calls from unwanted origin.
7. **Pre-testing**: Initial testing of device to prevent malwares and ensure security of various application and the device.
8. **Regular Update**: Regular updates of security issues and fixes from the manufacturer has to be rolled out.
9. **Remote access Control**: Remote access control is used when a user loses his/her phone and the user can remotely find his phone and access it. This is one of the major and important feature.

### 3.2 Types of attacks

Attacks are becoming really common in smartphones. A hacker constantly tries to steal a user's information and he is constantly trying to find loopholes in the security and finding ways to attack a user's phone. He would steal the private information such as passwords, user location, contacts etc. hacker would also steal saved credit card information and try to buy and make transactions online. A user needs to be really careful and protect his phone using some security measures and an Antivirus should be installed onto the smartphone.

| Title | Description |
|---|---|
| Data Leakage | If a smartphone is stolen or lost, an attacker can steal the information |
| Unintentional disclosure of data | A user may not want to disclose some data but he/she is forced to. |
| Attacks on decommissioned smartphones | Sometimes the user might not decommission the smartphone properly while selling. [11] |
| Phishing attacks | An attacker can steal personal information by many means. |
| Spyware attacks | An attacker can install spywares and it allows his to access personal information. |
| Network Spoofing | The attacker tampers the user communication |
| Surveillance attacks | An attacker keeps an eye on the user, even capturing the user's movements. |
| Diallerware attacks | The attacker steals money by forcing the user to send premium SMS |
| Financial malware attacks [9] | Some malwares steal information such as Banking details |
| Network Congestion | Attackers overload the network and cause a congestion. |
| Break-in | An attacker can gain partial or take full control of the target phone. |

**4. User ignorant on app permissions**

A user usually downloads these apps and while installing, the apps seek certain permissions which the user has to agree in order to install them, hence without reading these permissions the user readily clicks 'Next' and installs these apps. These permissions can be accessing of Camera, Phonebook etc. Some apps may not be free or may not be available in the Android Play Store and hence the user downloads it from various sites. These sites maybe malicious and they could infect the mobile phone. These apps could steal the users' location, passwords and even spy on the user.

Developments in Wireless mobile technology has brought people together across the globe. People from distant areas are able to connect to each other with just a handheld device called a mobile phone. Mobile phone was invented in the year 1973.It was commercially available in the year 1983.A mobile phone is a handheld device which is used to make and receive calls over a radio frequency carrier. The radio frequency link establishes a connection to the switching systems of a mobile phone operator, which provides access to the public switched telephone network (PSTN) [1].

A smartphone is a phone which can perform many features and they have an advanced operating system. These phones are usually touchscreen. These phones have various technologies and have GPS, Internet, Wi-Fi. Most smartphones produced from 2012 onwards also have high-speed mobile broadband 4G LTE internet, motion sensors, and mobile payment [2].

Most common Operating systems are Android, IOS, Windows, Ubuntu etc.

**4.1 Benefits**

If a user loses his phone, some applications can be used to track the location of the phone and the location can be shown on the maps. Apps like Whereas My Droid, Lost Android.

**5.Camera-Based Attacks on Mobile Phones**

There are certain apps on the android Play Store called spy cameras. There are nearly 100 spy camera apps, which allow phone users to take pictures or record videos of other people without their permission. Attackers can integrate these camera apps in other apps such that the phone camera is launched and a picture of the user or a video of the user is recorded. According to a survey on Android malware, the camera permission is in the 12th position among most commonly requested permissions among benign apps and it is out of the top 20 in malware. [3].

**5.1 Threats and Benefits of Spy Camera**

1.Stealing private information

Users some malicious apps without their knowledge and these apps on one hand performs the functions it claims and on the other hand it runs as a service in the background and uses the camera to take pictures and record videos.

2.Restrict unauthorized use of Phone

Users does not want other users to check their phone without their permission. So some apps can be used to take the picture of the user who inputs a wrong password to unlock the phone.

3.Anti-thief

When a user loses his/her phone the user can launch camera remotely and capture the photo of the thief.

### 6. Intruders in Android Applications

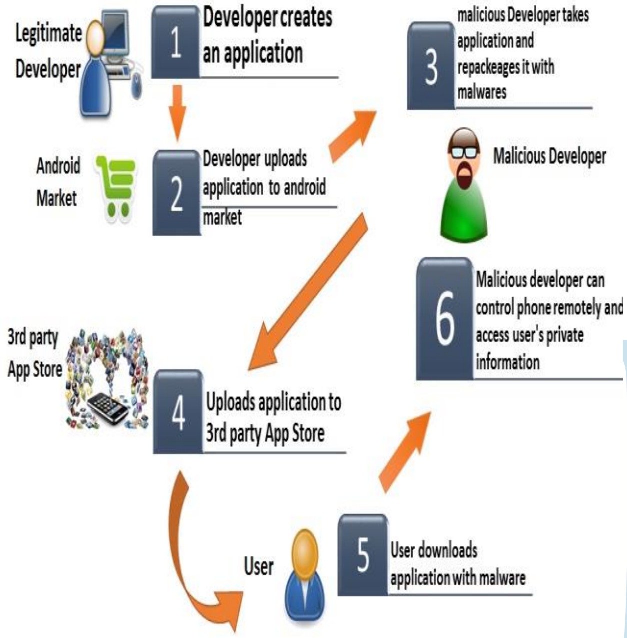
Legitimate Developer
1
Developer creates an application
Android Market
2
Developer uploads application to android market
3
malicious Developer takes application and repackeages it with malwares
Malicious Developer
6
Malicious developer can control phone remotely and access user's private information
3rd party App Store
4
Uploads application to 3rd party App Store
User
5
User downloads application with malware

Fig.4 shows how a Malicious developer can attack a phone.

1.A Developer creates and application based on the users' need.

2.The developer uploads the app into Android Market.

3.Malicious developer downloads the app and modifies it with malware.

4.The malicious developer uploads the app to 3rd party app store.

5.User downloads the app from the 3rd party app store.

6.Malicious developer can control the users' personal information, location, silently download malicious apps etc.

### 7.Conclusion and Future work

Various android security issues are analyzed. Focus on the security issues in a camera is a need due to high confidentiality. In future a novel approach to prevent android security attack on camera would be proposed and the effectiveness of same would be evaluated.

### References

[1] https://en.wikipedia.org/wiki/Mobile_phone

[2]https://en.wikipedia.org/wiki/Smartphone

[3] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," IEEE Symp. Security and Privacy 2012, 2012, pp. 95–109

[4] https://en.wikipedia.org/wiki/Firewall_(computing)

[5] Kaspersky Security Bulletin 2013. Overall statistics for 2013, https://www.securelist.com/en/analysis/204792318/Kaspersky Security Bulletin 2013 Overall statistics for 2013

[6] Google bouncer : Protecting the google play market, http://blog.trendmicro.com/trendlabs-security-intelligence/a-lookat-google-bouncer

[7] Android and security: Official mobile google blog, http://googlemobile.blogspot.in/2012/02/android-and-security.html

[8] McAfee Labs Threats Report: Third Quarter 2013, http://www.mcafee.com/uk/resources/reports/rp-quarterly-threatq3-2013.pdf

[9]Backdoor.AndroidOS.Obad.a, http://contagiominidump.blogspot.in/2013/06/backdoorandroidosobada.html

[10] Android Security Overview, http://source.android.com/devices/tech/security

[11] Smartphone: Information security risks, opportunities and recommendations for users,ENISA Report (December 2010)

[12]http://www.engineersgarage.com/articles/what-is-android-introduction

[13]https://en.wikipedia.org/wiki/Android_version_history