Rooting of Android Devices and Customized Firmware Installation and its Calibre

[1]Rahul Pal, [2]Randheer Kr. Das, [3]R. Raj Anand

Department of MCA,Veltech Multitech Dr.Rr Dr.Sr Engineering College, Chennai
[1] emailrahulpal@gmail.com, [2]mcarandheer@gmail.com, [3] rajsra_mca@rediffmail.com

Abstract-- ***When we use a mobile device which runs Android, we usually look for the basic features such as call, texting, gaming, internet browsing, camera and music. However Android devices can be made more powerful and its power can be utilized in a larger scale once it has been rooted.***

Keywords-- Root, Rooting, Android, Recovery, Bootloader, Overclock.

I. Introduction

This paper gives an analysis of a process called as “Rooting” which is not known to a large portion of the general public who use android devices and are yet unknown to the possibilities of numerous experiments which can be done with this open source operating system. When compared to the total number of people who use android devices on a regular basis, only a few know about the true potential of “Rooting” and how countless experiments have already been performed by many hard-core programmers and how they have made everything they worked on available to the general public, for FREE.

II.Methods and Methodology

What is Rooting?

Android rooting is the process of allowing the users of devices running Android mobile operating system to attain privileged control (known as “root access”) within Android’s sub-system.

Goals

Rooting is often performed with the goal of overcoming limitations that carriers and hardware manufacturers put on some devices, resulting in the ability to alter or replace system applications and settings, run specialized apps that require administrator-level permissions, or perform other operations that are otherwise inaccessible to a normal Android user. A user who has no technical knowledge about the sub-system of the operating system might make a few changes unknowingly which may prove to be fatal to the device. For this very reason perhaps, the manufacturers fix limitations on the access which a user gets over the device. And many believe that these limitations are too much and hence rooting was introduced. Rooting also facilitates the complete removal and replacement of the device’s operating system.

Android is derived from the Linux kernel, and hence, rooting an Android device gives similar access administrative permissions as on Linux or any other Unix-like operating system such as FreeBSD or OS X.

Rooting can not only be performed in Android devices, but also in other devices such as Nokia which used to run Symbian OS in most of its devices until the recent shift towards Microsoft Windows, and Apple devices which run the iOS. But when it comes to iOS (Apple devices), the term used for the process of rooting is JAILBREAKING. However, these concepts differ. Jailbreaking does not allow for OS replacements, instead it bypasses several Apple prohibitions for the end user.

Rooting : A problem for Manufacturers?

Many number of android device manufacturers have tried to implement severe security/protection features in their devices in order to make them “unrootable”. But unfortunately those devices were still managed to be rooted by the users in some way. There may not be any features available to root the recently launched devices but usually it’s available in a couple of months once a developer of modified operating systems gets his/her hands on the device and performs various experiments on it. In the year 2011, Motorola, LG Electronics, and HTC added security features in the hardware level to prevent users from rooting the stock Android OS which came with the devices as a retail package. The Motorola Droid X has a security boot-loader that boots the phone into “recovery mode” if the user loads an unsigned, i.e., modified Android OS that hasn’t been approved by the manufacturer. But, the developers have managed to come up with a way of upgrading the “boot-loader” itself into a different version and then moving on with the installation of unsigned operating systems without any problems.

What is Boot-loader?

Boot-loader is a piece of code that runs before any operating system starts running. Boot-loaders can be used to boot other operating systems. Usually, each operating system has a specific set of boot-loader codes. Since, it is the first software to run after a system’s power-up or reset, it is highly processor and board specific. Various manufacturers use various kinds of processors and chipset boards and hence they have specific boot-loaders for different models of their devices.

Android Architecture and Security

Android seeks to be the most secured and usable operating system for mobile phones (smartphones and tablets). Having the Linux kernel makes it a well secured operating system but as Android keeps upgrading and becomes more and more enhanced with added features, it also faces security threats and these security issues keep growing with time. The stock version of the OS provided by the device manufacturer limits the root access to the users and it is a well thought security threat prevention scheme. If the administrator (the user) itself doesn’t get the root access, then the applications installed by the users which if infected by a malicious file cannot harm the core of the Android in the device. As per the architecture, the Linux kernel consists of the display driver, the camera driver, flash memory driver, Inter Process Communication driver, Keypad driver, Wi-Fi driver, Audio drivers and Power Management. The device can be seriously harmed if any of the above mentioned drivers get affected. Android applications do consist of anti-virus apps which help a lot. But, if the Android device is rooted, it gives flawless access of the root-files and the kernel to the user and this means any application installed by the user will get the access to the root files. Under such circumstances, the device becomes seriously vulnerable to security threats and the user must be very careful about the applications the user decides to install. Any small irresponsibility by the user can brick the device and the use might have to go through a long procedure of re-rooting the phone and installing a new bootloader and then the operating system and lose all data in the process.

The users tend to rely on smartphones with sensitive data such as Bank Account details, contacts and address books, documents and media files such as pictures and audio/video data. Losing all the data is always a risk in rooted devices and the manufacturers will take no responsibility as rooting voids any warranty applicable to the device.

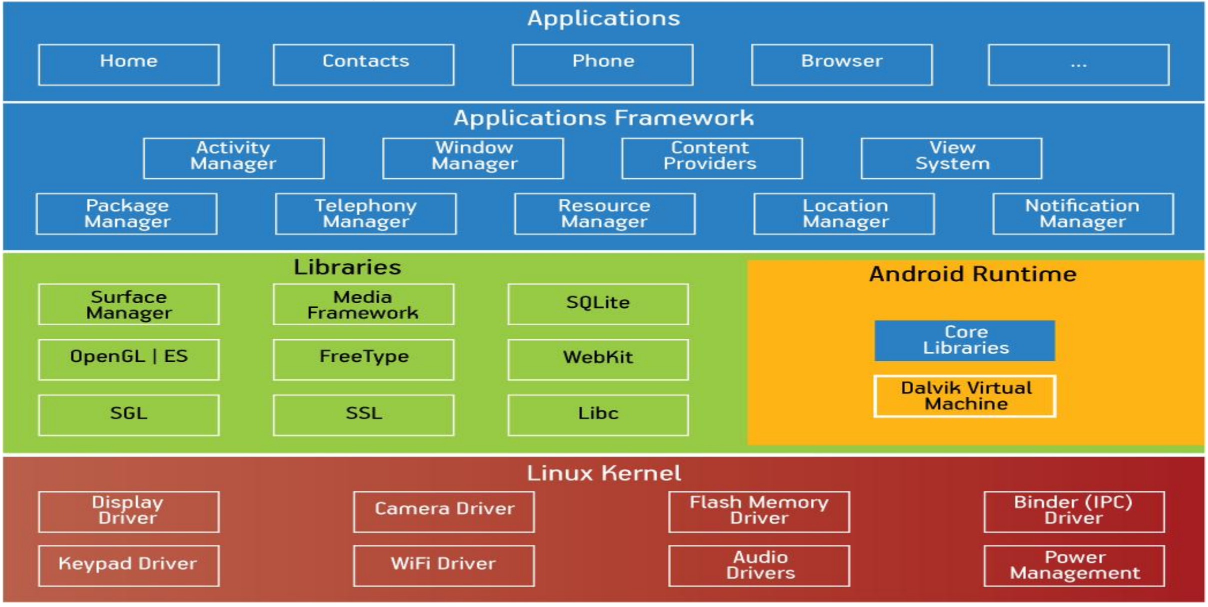


Fig.1 Android Architecture

Rooting Procedure

There are different ways to root a mobile device. Various software tools are available in the internet to perform rooting and installing "SuperUser" app to provide complete access of the root files to the users, in other words, making the user a Super User. These tools are free of cost and are also capable of unrooting a mobile device. If a user decides to root a phone which still happens to be under warranty period and runs into some error during the process, the user will lose the warranty. However, the users can use these tools to unroot their devices and the manufacturer will never know that the device has gone through a rooting procedure. Another way (the complicated way) to perform rooting is to manually flash the mobile devices using flashing tools and install zip files from the recovery-mode of the devices and then get root access. The user must remember that in order to perform these operations, the bootloader of the device must be unlocked. This process of rooting varies from one device to another. Even though the process varies, the main objective of exploiting security bugs in the stock Android OS remains the same in all the processes. Once this exploit is discovered, a custom recovery image is flashed which skips the digital signature check of the stock firmware updates. Then a modified firmware update can be installed from the recovery menu which typically includes the utilities required to run apps as root. These firmware updates can otherwise also be a customized Android OS. They are usually compressed into a single file with a .zip extension. This .zip file is stored into the external SD memory card. When the user enters the recovery menu, the user must clear cache partition and Dalvik Cache (from inside Advance menu) and then select "install .zip from card" and this will show the .zip file to the user, which when selected starts the installation process. The user must keep the mobile device charged to 80% battery level (at least). During the installation process, every process including the power management featured from the kernel is replaced with the kernel of the customized OS and hence the mobile device doesn't charge its battery even though the device is connected to the computer or a power supply.

Various Processes for Various Devices

The process of rooting a device may be simple or complex, and it even depends upon the device. Although the process is comparatively similar, it is however complicated when it comes to some devices (Sony and Samsung for example). But, rooting is like a one time investment. Once a device is rooted successfully, various customized operating systems can be installed any number of times and no rooting process has to be performed unless the device has been unrooted. The user has to install the drivers of the device in the computer before starting the rooting process. If the user doesn't install the drivers, the computer will not recognize the device and as a result the flashing tool will fail to flash the file with roots the device. In order to root Samsung devices, the users have to install a tool called Kies which includes the drivers for the devices. After this the users have to install a tool called Odin which is the flash tool for Samsung Devices. Odin allows the user to flash the recovery menu along with the SuperUser app which roots the device. After this the users get an extra option named

"Advanced" in the recovery menu where the user can clear the Dalvik Cache partition and install the customized operating system (.zip extension) from the SD card which the user has to copy in the SD card before starting the rooting operation. The entire process takes 10 to 20 minutes.

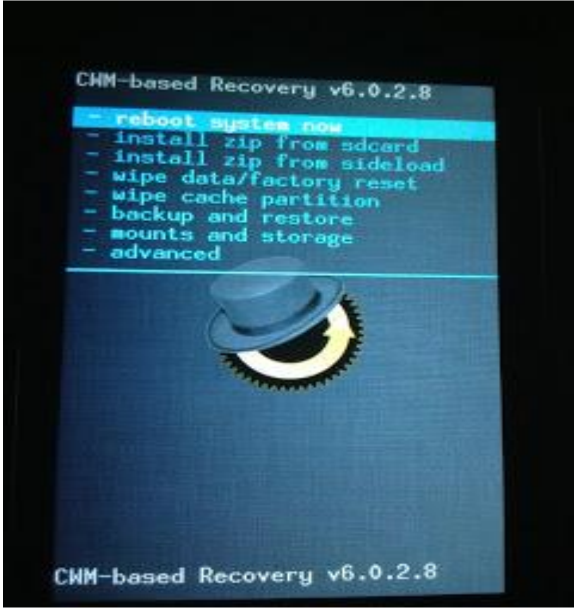

CWM-based Recovery v6.0.2.8
- reboot system now
- install zip from sdcard
- install zip from sideload
- wipe data/factory reset
- wipe cache partition
- backup and restore
- mounts and storage
- advanced
CWM-based Recovery v6.0.2.8

Fig 2. CWM Recovery Menu of Samsung

Similarly, for Motorola devices, the users have to use a tool called RSD Lite which is the flash tool for Motorola. The extension of recovery menu and the firmware vary for different devices. The firmware extension for Motorola devices is .sbf, which the users must download for their respective device models and flash it using RSD Lite. This process takes almost 20 minutes after which the mobile device reboots itself. Once the device reboots, the user has to switch off the device and turn it on with a specific key combination (power+volume down keys for Motorola Defy) which lets the user enter the recovery menu. Once the users get inside the recovery menu, the procedure to install the customized operating system is same as Samsung. The user has to clear the partitions and install the .zip file from the SD card.

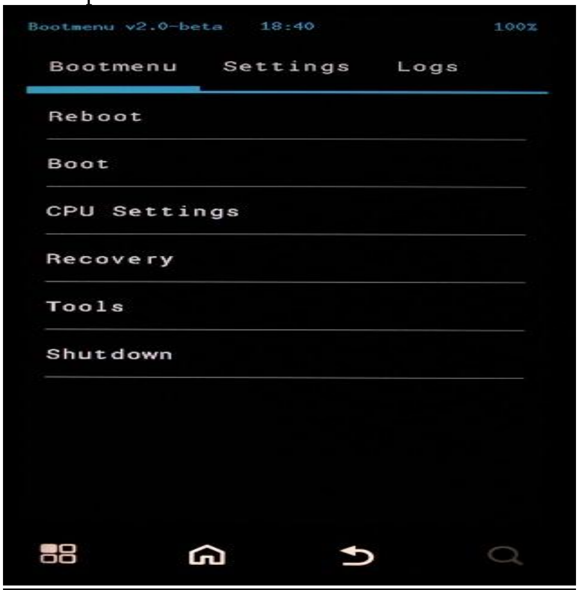
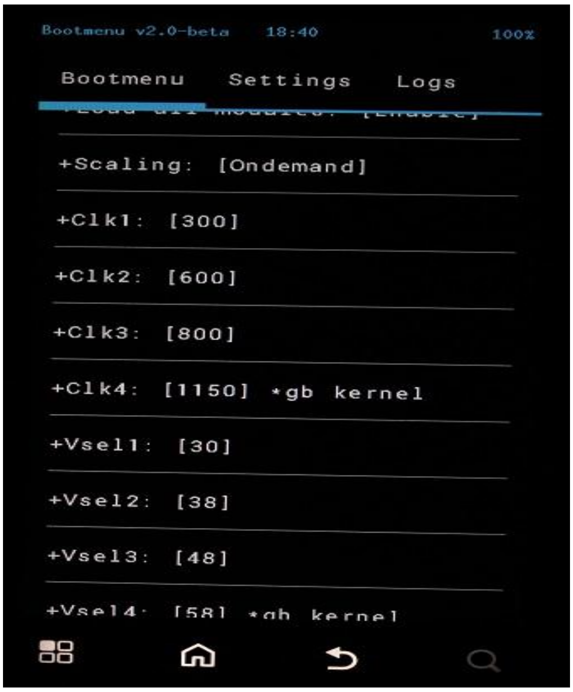


Fig 3 Motorola(Defy+) Rooted Recovery Menu

CPU Overclocking

Rooting a mobile device not only provides root access to the user but the rooted recovery menu gives an additional option called the CPU Settings where the users can modify the settings of the CPU and overclock it to process faster than usual. For example, a Motorola Defy+ android device comes with a dual core 1GHz processing unit, but the users can overclock it to 1.1GHz or 1.2GHz and make it run faster than usual. This however has a minor negative effect of using a little extra power from the battery.



+Scaling: [Ondemand]
+Clk1: [300]
+Clk2: [600]
+Clk3: [800]
+Clk4: [1150] *gb kernel
+Vsel1: [30]
+Vsel2: [38]
+Vsel3: [48]
+Vsel4: [58] *gb kernel

Fig 4. CPU Overclocked Settings

III. Results

The results of rooting an Android devices are astonishing. However, since the rooted firmware of various manufacturers are developed by various programmers who do not necessarily work in a mobile manufacturing industry, the programmers do not always develop a stable ROM. Many of the customized operating systems available online are marked as UNOFFICIAL and this usually means the ROMs may have some bugs which haven't been debugged. But, there are some OFFICIAL/STABLE ROMs available which happen to work far better than the stock operating systems as per various user reviews. The users who have successfully rooted and installed customized Android systems in their devices have reported it to be extremely efficient and powerful. The users have noticed a slight improvement in performance after overclocking their devices' CPUs. Some devices such as the Motorola Defy which was discontinued in the Indian market a while ago had their support limited only till Android's GingerBread version. However, a rooted Motorola Defy is capable of installing customized operating system based on the firmware of Android JellyBean and KitKat which happens to be the latest version of Android. The users have noticed a huge improvement in RAM usage and power consumption as well. Users haven't faced any security threats from the stable customized ROMs so far.

IV. Conclusion

In this paper, we have discussed about the process of Rooting an Android device and we have given an insight of how resourceful and efficient a customized ROM based on Androids kernel and firmware can be. Irrespective of some drawbacks, these custom ROMs prove to be worthy operating systems and have the potential to perform really well if they get the proper support at the right time. If the mobile manufacturers at some point consider combining their development teams and the developers of the customized ROMs, they can produce multiple operating systems that would suit a wide segment of users who would prefer various operating systems based on their priorities.

Acknowledgement

The author wishes to acknowledge Vel Tech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College (Affiliated to Anna University) for providing grateful support and necessary help for the work that has been done in this paper.

References

i. Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh (19th November,2013) “Review on Android and Smartphone Security”.

ii. "CyanogenMod supported by Samsung" January 16, 2012

iii. Official Bootloader Unlock Instructions

iv. The Official AT&T FAQs

v. Does rooting your device (e.g. an Android phone) and replacing its operating system with something else void your statutory warranty, if you are a consumer? (fsfe.org/freesoftware/legal/flashingdevices.en.html)

vi. "Is It Illegal To Unlock a Phone? The Situation is Better - and Worse - Than You Think | Electronic Frontier Foundation". (https://www.eff.org/is-it-illegal-to-unlock-a-phone)

vii. Wikipedia (Android Rooting)

viii. “Motorola Offers Unlocked Bootloader Tool” (techcrunch.com/2011/10/24/)

ix. “MIUI is popular” (androidandme.com)

x. www.miui.com/en

xi. “What you can do after rooting your Android device”, Gaurav Gahlyan (www.droidiser.com/2012/11/what-after-rooting-apps-tips.html)

xii. Source.android.com