Android Rooting and Customization

Devarsh Anilbhai Shah[a]*, Madhuri Chopade[b]*

[a]*M.E. Scholar, Gandhinagar Institute Of Technology, Motibhoyan, Gandhinagat, India*

[b]*Assistant Professor, Gandhinagar Institute of Technology, Motibhoyan, Gandhinagar, India*

Abstract

Android is today’s most popular operating system and is used worldwide and because of this it has wide area of users, so as user increases customization also increases. If we look back Android has amazing journey from Android Donut Version 1.6 to Android 11 with many changes in the operating system from version to version. As for security reasons operating systems restricts user to perform some advanced task or customization so to overcome these developers have made some special customization which we can apply and can become Super User. This paper is going to tell everything about Android Customization and how to perform in certain Android mobile. Custom Rom are developed in which a user becomes a Super User and can-do customization as needed.

Keywords: Android, Operating System, SuperUser, Customization, Custom Rom.

1. Introduction

When comparing with the other operating systems in the market we can see that there are many choices available, for example Android, iOS, Windows Operating Systems. But when comparing in customization amongst the OS, Android is most widely preferred as it is the modified version of Linux Kernel and most importantly it is Open Source which means it is completely free of cost and can be accessible throughout the world. The term “Customization” means to develop something different from what it is originally shipped from the factory. In this paper the thorough process of what is needed, what are the merits and demerits of this techniques and what are the risks involved in this will be covered.

1.1. Prerequisite

Android is a deep sea if looked according to developers as it is highly customizable. For this there are prerequisite, if requirement does not match then there are highly possible chances of getting device bricked. First thing is that after performing this task your phone will be out of warranty so make sure that phone is already out of warranty.

- Step-1: Mobile device must be rooted.
- Step-2: Bootloader should be unlocked.

If these two steps are done for the device, then we can go further for the Custom Recovery (TWRP) Installation, Custom Rom installation and applications. There are certain definitions which will be covered in this paper.

1.2. Definitions

1) **Android:-**Android is a mobile operating system based on a modified version of the Linux kernel and other open source software, designed primarily for touchscreen mobile devices such as smartphones and tablets.[1]
2) **Rooting Android:-**Rooting is the process of allowing users of the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems.[2]
3) **Stock Recovery:-**Stock recovery is the recovery which comes pre-installed with the operating system and which is restricted to perform superuser permissions.
4) **Custom Recovery:-**Team Win Recovery Project (TWRP) is an open-source software custom recovery image for Android-based devices and provides a touchscreen-enabled interface that allows users to install third-party firmware and back up the current system which are functions often unsupported by stock recovery.[3]
5) **Bootloader:-**The bootloader runs on device start-up and is in charge of loading the operating system on the phone. It is generally in charge of verifying that phone system information hasn't been tampered with and is genuine.[1]
6) **Root Checker**:- It is an application which verifies that whether root permissions are properly installed or not. There are various root checker applications which are available on the Google Play Store which can be downloaded into the device freely.

*Devarsh Anilbhai Shah
E-mail address: devarshshah1999@gmail.com

7) **Stock Rom:-**Rom which comes pre-installed with the android device and it is proprietary to the makers of the devices and customization is not possible in this kind of rom as restriction are there for the user to perform superuser tasks.
8) **Kernel:-**The kernel is a computer program at the core of a computer's operating system that has complete control over everything in the system. It is the "portion of the operating system code that is always resident in memory" and facilitates interactions between hardware and software components.[4]
9) **Custom Rom:**-Custom rom's are quite different from the stock rom's as this are made keeping in mind to give full access to the user of the android and doing customization as per needs. Here all superuser permissions are accessible as this is a custom rom.
10) **Firmware:**- In computing, firmware is a specific class of computer software that provides the low-level control for a device's specific hardware. Firmware can either provide a standardized operating environment for more complex device software (allowing more hardware-independence), or, for less complex devices, act as the device's complete operating system, performing all control, monitoring and data manipulation functions. Firmware is held in non-volatile memory devices such as ROM, EPROM, EEPROM, and Flash memory.[5]
11) **Dalvik Cache:**- Dalvik is a discontinued process virtual machine (VM) in Android operating system that executes applications written for Android.[6]
12) **Flash Memory:**- Flash memory is an electronic non-volatile computer memory storage medium that can be electrically erased and reprogrammed.[7]
13) **ADB:**- The Android-Debug-Bridge (abbreviated as *adb*) is a software-interface for the android system, which can be used to connect an android device with a computer using an USB cable or a wireless connection. It can be used to execute commands on the phone or transfer data between the device and the computer.[8]
14) **Fastboot:**- *Fastboot* is a protocol and it has a tool with the same name included with the Android SDK package used primarily to modify the flash filesystem via a USB connection from host computer.[9]
15) **USB Debugging:-** The main function of this mode is to build a bridge between an Android device and a computer with Android SDK (Software Development Kit) which is a development platform for the developers to design and test their Android apps and mods.[10]
16) **GApps:-** GApps stands for Google Application and it is vital file for any custom rom as it contains the basic application which are provided from the google like Phone, Contacts, Messages, Camera, YouTube, etc.

2. Literature Survey

2.1 Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics.
Author: - Almehmadi, T., & Batarfi, O.
In this paper the author have explained about the main root cause and how big the challenges are when the rooted android is hacked, furthermore they have described about the Data Integrity of the user which is being compromised on an Android Rooted device if proper care of data is not taken.[17]

2.2 Rooting Your Android Device.
Author: -Sheran Gunasekera.
In this paper the author has described the advantages and disadvantages of the rooting android in fully fledged emulator and just shown the working process of how rooting can be done in specific android device, furthermore they have talked about why to root your device and what are the risks hidden behind it.[18]

2.3 Rooting of Android Devices and Customized Firmware Installation and its Calibre
Authors: - R Pal, RK Das, RR Anand.
In this paper they have talked about general trivia of what Android mobile phones are capable of, for example Call, Music, Gaming, etc. They have also talked about the information about what is recovery and how it is very useful when dealing with rooting process and also a rough idea on Overclocking the CPU of an Android Device.[19]

2.4 Android Rooting and Risks Involved.
Author: - Vishal Gaikar.
In this paper the author has talked about the rooting process in Tablet and what sort of recoveries are available in the market for the tablets and how it can be implemented in the Tablet, furthermore paper describes about the administrative rights which are available only after the rooting process is successful. Author has also given a general trivia on Computer based rooting process and gaining access root. In the advantages section this paper describes about the firmware access which are the core files of any Android Operating System which can be edited as per the user requirements. Lastly paper describes about the stability issues found in the device which might come if the process of rooting is not done properly and various other terms related to the performance of the Android Device.[20]

3. Installation Process

3.*1. Device Rooting Process*

For this paper I have taken Xiaomi Mi4i Android Device for rooting and installation of the rom. For this there are numerous ways to execute the plan but as for this paper I have taken toolkit.zip file for rooting the device [12], TWRP(Team Win Recovery Project 2.8.6.0) Custom recovery[12], crDroid Nougat 7.1 Custom Rom.[12], GApps 7.1[13].
Here is the step-by-step guide for rooting the Mi4i device.

- **Step-1: -** Make sure that you have got your backup from the device.
- **Step-2: -** Download the required USB Drivers from the internet depending upon the device.
- **Step-3: -** In device go to Setting icon-> About Phone -> Tap MIUI Version 7-8 times and you will become developer.
- **Step-4: -** In device go to Setting icon-> Additional Settings-> You will find Developer Options.
- **Step-5: -** After enabling Developer Options, inside it turn on USB Debugging option.
- **Step-6: -** Now connect the device to the computer/laptop through original USB cable.
- **Step-7: -** Unzip the file toolkit.zip on your computer/laptop.
- **Step-8: -** Make sure to keep all the extracted files in one folder.
- **Step-9: -** Open Start.bat file.
- **Step-10: -**Select option 1 from the list and hit enter, wait for the process to complete.
- **Step-11: -**Once the process is completed the device will reboot and SuperSu application will be installed on the device.

3.2. Installing TWRP Recovery

TWRP stands for Team Win Recovery Project and it is open-source custom recovery image for Android Devices and there are various versions which are available over the internet for almost all Android Devices, as of now for me I have installed TWRP custom recovery image version 2.8.6.0.
Here is the step-by-step installation guide for TWRP custom recovery image.

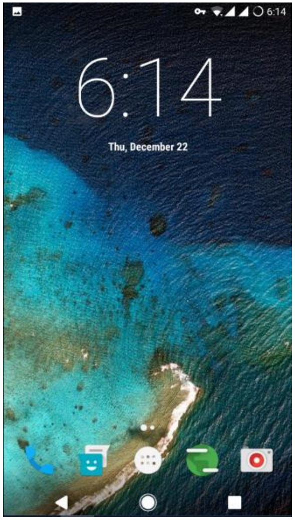
- **Step-1: -**Make sure that the device is rooted.
- **Step-2: -** In device Tap Setting icon-> About Phone -> Tap MIUI Version 7-8 times and you will become developer.
- **Step-3: -** In device Tap Setting icon-> Additional Settings-> You will find Developer Options.
- **Step-4: -** Now connect the device to the computer/laptop through original USB cable.
- **Step-5: -**Unzip the file toolkit.zip on your computer/laptop.
- **Step-6: -** Make sure to keep all the extracted files in one folder.
- **Step-7: -**Open Start.bat file.
- **Step-8: -**Select option 2 from the list and hit enter, wait for the process to complete.
- **Step-9: -**Once the process is completed the device will reboot.
- **Step-10: -**In the device go to Setting icon-> About Phone-> Check Updates-> Click upper right hand three dots-> Click Reboot to Recovery.
- **Step-11: -**The device will reboot into the recovery mode and you have successfully installed TWRP Recovery.

3.3. Installing Custom Rom and GApps

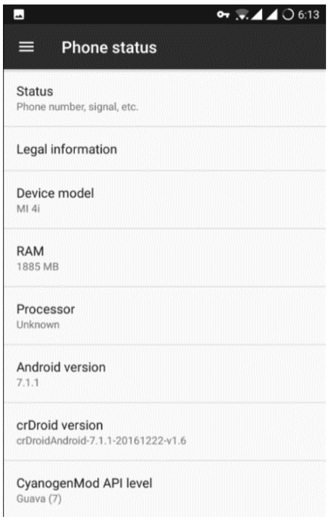
Custom rom or Custom firmware is something like giving Android a new shape in one own's perspective, for example after a period of time Mobile Companies stop pushing the updates to the devices like going from one Android version to another (Android 5.0 to Android 6.0). To overcome this customization takes place where a unsupported device can also go to the higher version of Android by some tweaks. Talking about GApps it goes from the version to version and also from size to size for example if you want only basics application to run on the android then select the Pico version from the tab and hit the download button which will automatically download a zip file which can be later installed in the recovery and if you want each and every application from google to run on your device then download Full version from the tab and save it in the computer/laptop which again will be used later in the installation process.
Here is the step-by-step installation process for the Custom rom/firmware.

- **Step-1: -**Download the required custom rom/firmware and GApps from the internet for the device.
- **Step-2: -**Place it in the mobile's internal storage folder name downloaded_rom.
- **Step-3: -**First do a Android Backup using TWRP Recovery.
- **Step-4: -**For this go to recovery mode by tapping some dedicated button's combination or through the system update.
- **Step-5: -**Tap on Backup button then select System, Data, and Boot to make a complete backup of your current rom.
- **Step-7: -**Go back to main screen of TWRP recovery and click on Wipe button.

- **Step-8: -**Do a Factory Reset.
- **Step-9: -**Again tap on the Wipe button and select Advanced Wipe button.
- **Step-10: -**Select Dalvik Cache, System, Cache icon and wipe the selected.
- **Step-11: -**Go back to main screen and click on Install button.
- **Step-12: -**Select both the files (Custom rom and GApps) which was kept in downloaded_rom folder and then confirm flash.
- **Step-13: -**Wait for the process to complete and once it is completed, select reboot.
- **Step-14: -**Initial boot may take several minutes but don't worry it will boot.
- **Step-15: -**Complete the initial startup process and voila! you have successfully installed Custom rom/firmware and GApps on your device.



(A)


6:13

Phone status

Status
Phone number, signal, etc.

Legal information

Device model
MI 4i

RAM
1885 MB

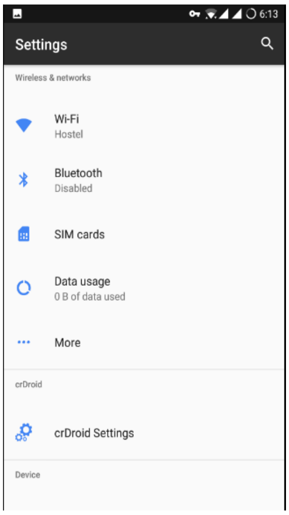
Processor
Unknown

Android version
7.1.1

crDroid version
crDroidAndroid-7.1.1-20161222-v1.6

CyanogenMod API level
Guava (7)

(B)


6:13

Settings

Wireless & networks

Wi-Fi
Hostel

Bluetooth
Disabled

SIM cards

Data usage
0 B of data used

More

crDroid

crDroid Settings

Device

(C)

Fig-1 crDroid Main Screen(A).

Fig-2 crDroid Phone Status Screen(B).

Fig-3 crDroid Settings Screen(C).

4. Advantages And Disadvantages of Rooting Android

4.1. Advantages of Rooting Android

There are lots of advantages of rooting Android, rooting gains the access of the Super User through which user becomes inevitable as they can run any kind of program they want to run on the device. Rooting has also capabilities to remove system applications which comes pre-installed in the mobile. It has also capabilities of running special applications which are specially made for root users and which are mostly available over the internet but some of the applications like File Checker Root Explorer, Root Checker are officially available in Google Play Store. Through some tweaks you can also install complete applications into SD card if mobile supports SD card slot which can be a lot helping hand in freeing up the internal storage space in handset. Mobile becomes durable for longer period of use because when manufactures stops giving updates to phone but still through custom rom you can update to the latest version of the Android. After rooting Ads are also removed/blocked instantly from any applications or games same as like computer/laptop browser. User can access the main Android core files (root files) in which the complete programming is done of the operating system and can also edit, update or delete the files from the same. The main advantage through rooting is one can Clock the speed of the CPU (Central Processing Unit) like over clock the CPU for getting maximum power from the Chipset and same ways under clocking the speed to extend the better life of the chip, application like No Frills CPU Control can do these things with ease and which is freely available on Google Play Store and there are many more applications which can do these things available over the internet. After rooting the Android there are infinite number of tweaks available over internet for customization and optimization for the handset.

4.2. Disadvantages of Rooting Android

In this world nothing is 100% perfect so but obvious rooting your handset have equally disadvantages which may or may not affect to the user directly, so if user is new to rooting then this is a pretty arduous task to accomplish and without any problems. The main disadvantage of rooting Android is bricking the device. Brick device meaning if any of the task is missed or any corrupt file is flashed then the device is unusual for sure and it is called brick, to overcome this type of issue there are 2 ways, one is to go to the manufacture's service center to fix the issue and second doing it by yourself. One more main issue after rooting is the warranty will void for sure once you successfully root the device. It is amazing to have the super user access but this kind me tricky for some of the users as if you misplace some core Android file or update or delete the files then this can end up into some serious trouble and in end making it unusual. Another problem related to rooting is tweaking risks, so if the user flashes wrong kernel or wrong custom rom which is not made for the device in the first place then this can create major issues with the device and either two things can happen one is bricking the device and second is nothing will happen. Regarding the updates to the device no matter ho long it takes for the manufactures to build the updates for the device but if they are supporting the device then for surely the update will come to the device, but if device is rooted then this can be messy as the updates will no longer come to the devices or if it comes then may not install as device is registered with different recovery. Talking about the ad blocking in the device then this is a big advantage for the user but disappointing for the developers as they make revenue from the ads which are showing to the user and if user stops this then at some point of time developers have to discontinue the project which makes the application or game useless as no further updates/fixes will be provided from the developer end and in the long time it affects the user only as after a period of time because of the errors in the application will stop using it and deleting it from the handset.

5. Risks Involved

5.1. Risks in Customization

Up to this far we have talked about what is Android rooting, how it is done and what is customization in android and also advantages and disadvantages of it. Now let us see what are the risks involved in this practice. First and major risk is that at some point of time if the file is corrupt and if tried to flash then the device will be bricked and completely unusable. Secondly is the cost and time effort needed in this kind of work if something goes wrong in the installation process. Thirdly in recent events because of demanding in Android customization, manufacture's locks the devices bootloader and can only be unlocked by requesting to unlock the same to the manufacture, giving them valid reason that why they need bootloader unlocked and sadly there is no other way to overcome this problem so if user is rejected for the permission, then they need to apply again and again until company gives the authorization. Fourthly, there is no security kind of thing in this kind of practice so the device with root access and custom rom installed becomes highly vulnerable to the threats, so there is no such think called privacy in the handset. If device gets the virus or is hacked then there is no way to overcome from this kind of situation unless to change the rom or doing a hard factory reset. Customization can also be risky if the core tweaks application is not used properly as this may degrade the performance of the device and even worse, over heating of the device causing to shut down the system forcefully, because of this the life span of the device may reduce drastically and end up into becoming an e-waste.

6. Conclusion

Android is excellent platform for customization but comes with great responsibilities and prize, so be clear as in this paper both pros and cons are discussed so it is up to the user that is this worth doing it or should walk away from this kind of practices whether it is worth taking the risk for the same or not and if answer is yes then user must be thoroughly clear about the customization process as a single mistake can take the life away from the device. There is plethora of techniques available over the internet doing the same thing but with different tools and technologies so for future implementation of this practice it can be done without need of unlocking the bootloader.

References

1. Nimodia, C., & Deshmukh, H. R. (2012). Android operating system. Software Engineering, 3(1), 10.
2. Chinetha, K., Joann, J. D., & Shalini, A. (2015). An evolution of android operating system and its version. International Journal of Engineering and Applied Sciences, 2(2), 257997.
3. Wu, S., Xiong, X., Zhang, Y., Tang, Y., & Jin, B. (2017, October). A general forensics acquisition for Android smartphones with qualcomm processor. In 2017 IEEE 17th International Conference on Communication Technology (ICCT) (pp. 1984-1988). IEEE.
4. Gilski, P., & Stefanski, J. (2015). Android os: a review. Tem Journal, 4(1), 116.
5. Alure, S., & Puri, R. (2021). FIRMWARE DESIGNING FOR ANDROID MOBILE. INTERNATIONAL JOURNAL, 5(12).
6. Welton, R. (2015). Remotely abusing android. Black Hat London 2015.
7. Al-Rayes, H. T. (2012). Studying main differences between android & linux operating systems. International Journal of Electrical & Computer Sciences IJECS-IJENS, 12(05), 46-49.
8. Kobayashi, T. (2012). ADB (Android Debug Bridge): How it works?. Android Builders Summit.
9. Yang, X., Shi, P., Sun, H., Zheng, W., & Alves-Foss, J. (2016). A Fast Boot, Fast Shutdown Technique for Android OS Devices. Computer, 49(7), 62-68.

10. Lu, H., Helu, X., Jin, C., Sun, Y., Zhang, M., & Tian, Z. (2019). Salaxy: Enabling usb debugging mode automatically to control android devices. IEEE Access, 7, 178321-178330.
11. YUDHYA, D. T. B., & SE, M. (2017). THE INFLUENCE OF BRAND IMAGE, TRUST, PRODUCT AND PRICE TOWARD BUYING DECISION XIAOMI MI 4I AT BANDUNG ELECTRONIC CENTER (BEC), BANDUNG, WEST JAVA, INDONESIA. In Academic International Conference on Social Sciences and Humanities (p. 26).
12. Boueiz, M. R. (2020, June). Importance of rooting in an Android data acquisition. In 2020 8th international symposium on digital forensics and security (ISDFS) (pp. 1-4). IEEE.
13. Zhang, Z., Wang, Y., Jing, J., Wang, Q., & Lei, L. (2014, July). Once root always a threat: Analyzing the security threats of android permission system. In Australasian Conference on Information Security and Privacy (pp. 354-369). Springer, Cham.
14. Chen, Y., Zhang, Y., Wang, Z., Xia, L., Bao, C., & Wei, T. (2017). Adaptive android kernel live patching. In 26th USENIX Security Symposium (USENIX Security 17) (pp. 1253-1270).
15. Hay, R. (2017). fastboot oem vuln: Android bootloader vulnerabilities in vendor customizations. In 11th USENIX Workshop on Offensive Technologies (WOOT 17).
16. Ponakala, R., & Dailey, M. N. (2020). LineageOS Android Open Source Mobile Operating System: Strengths And Challenges.
17. Almehmadi, T., & Batarfi, O. (2019, May). Impact of android phone rooting on user data integrity in mobile forensics. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.
18. Gunasekera, S. (2020). Rooting Your Android Device. In Android Apps Security (pp. 173-223). Apress, Berkeley, CA.
19. Pal, R., Das, R. K., & Anand, R. R. (2014). Rooting of Android Devices and Customized Firmware Installation and its Calibre. International Journal of Scientific Engineering and Technology, 3(5), 553-556.
20. Gaikar, V. (2013). Android Rooting and Risks Involved.