ANDROID ROOTING: METHOD, BENEFITS and THREATS

Manjinder Singh
Assst Professor (Computers Department)
Heis-Govt Ranbir College Sangrur

Abstract

Rooting is the process of allowing users of smart phones, tablets and other devices running the Android mobile operating system to gain root access over various Android subsystems. Rooting is often performed with the goal of overcoming limitations that hardware manufacturers put on some devices. Thus, rooting gives the ability to alter or replace system applications and settings, run specialized "apps" that require admin-level permissions, or perform other operations that are otherwise inaccessible to a normal Android user. On Android, rooting can also facilitate the complete removal and replacement of the device's operating system with the latest custom ROMs. In this paper various things about Android Rooting, obtaining Superuser permission, switching from stock ROM to custom ROM have been discussed. It focuses on things like what is a Rooting, stock ROM, custom ROM, Methods of rooting device and installing a custom ROM by removing its default stock , what are the benefits and threats of installing custom ROM by removing its original stock ROM.

Keywords: Rooting, Custom ROM, Stock ROM, Custom Recovery

Introduction

Android is the mobile operating system developed by Google. Android is a Linux-based software system, and similar to Linux, is free and open source software. One of the most widely used mobile OS these days is ANDROID. Android is also associated with a suite of proprietary software developed by Google, called Google Mobile Services (GMS) that very frequently comes pre-installed in devices, which usually includes the Google Chrome web browser and Google Search and always includes core apps for services such as Gmail, as well as the application store and digital distribution platform Google Play, and associated development platform.[1]

Types of ROMs:

Android provides a rich application framework that allows you to build innovative apps for mobile devices. The stock ROM comes installed on the phone while a Custom ROM comes from a third party. The Custom ROM provides better features, frequent updates, and bug fixes and also in cases of some device you can even upgrade to a new version of Android which you may not if you are running on the Stock ROM made by the manufacturer. There are two types of

ROM‟s available for the android devices such as Stock ROM and Custom ROM described below:

Stock ROMs are the ones which come by default in Android phones. These are customized versions of Android done by mobile companies to make their devices unique in looks and features. The out-of-the-box smart phones are all shipped with stock ROM. Main Advantages of Stock ROMs are kept the warranty, pre-installed app, premium features and trust for security.[12]

Custom ROM is an aftermarket firmware which is a standalone OS and includes everything as in the stock firmware. A Custom ROM breaks the barrier between the user and the amount of customizability that every Android device holds. It allows the user to be much more precise and specific while using an Android device.[12]

Android Rooting:

Root refers to the administrative access to the system files on your Android device. In simple words, it means once you are rooted, you can access (and modify) those system files that are usually restricted by the OS. Well, there are various reasons for that, some of them being: You might want to change the appearance of your device. You might want to remove some apps that have come preloaded on your device. You might want to do some tricks with your phones. On the other hand, one of the main disadvantages of rooting a device is lacking the warranty. If you root your device, your warranty gets voided and the only way to get it back is to unroot your device. Unrooting refers to the process of removing root from your device and it is NOT possible to unroot all available devices. Clockworkmod recovery is the original custom recovery that is developed by Koushik Dutta and is the most popular recovery of all (arguably).There are three several CWM recovery are available for the devices, such as Standard version which uses hardware keys for navigation and selection, Swipe version which uses basic up/down/left/right swipe gestures to navigate and select options and the Touch version which is entirely touch-driven. Your first task is to power down your Android device and boot into the recovery mode which is different with different devices. You can either search for the hardware button combo in the Google or use any 3rd party apps (requires root) which do the same job.

Superuser

"Superuser" is used to manage applications which are allowed to gain root access. Superuser or SuperSu app grants you "root access") to run or install specific app restricted by the Android Operating System for a security concerns.

Some unofficial Android applications needs root permissions to access the core libraries of the Android Operating System. So we need to root the Android device and install Superuser app to manage root permissions.

su (short for Switch User) is a binary executable. It's used by Android and other *nix based systems to allow a process to change the user account it is associated with. The reason it's important from a rooting standpoint is that su without any other parameters will switch to the root user, meaning that processes that require root permission for their functionality need to invoke su(since by default they are not being run by root).

Superuser is an Android application. It works as a sort of "gatekeeper" to the su binary. Applications which attempt to invoke su will be forced to route through Superuser, which will then prompt the user if it is an unknown or new application. The user then has the option of approving or denying the access to su and optionally having Superuser remember their decision so it can automatically apply it for subsequent calls by that app. By doing this, the only apps which are granted root permissions are ones that the user chooses. The source of both applications is available on Github.[3]

Method OF Android Rooting and installing custom ROM:

One can root any android device, gather Superuser access right then flash any custom ROM in that device. We can flash any ROM in any device provided the specification of device should support the ROM specifications; otherwise some features may not work properly. The process of installing custom is:[11]

- Android device.
- Unlocking bootloader.
- Installing custom recovery.
- Open recovery mode.
- Wipe all data.
- Wipe dalvik cache.
- Move to storage where Rom zip file is stored (pen drive preferred).
- Flash ROM file.
- Once done reboot.
- Install and grant supersu for root access.
- Install some rote checker apps to verify root access.

Rooting this device is actually quite a simple and easy process. Before you begin, it is recommended that you at least try to understand what each part of the process will do and the whole process is specific for “ONEPLUSONE” MOBILE. Although this guide will describe each step in order to show all of the details, the method used can be broken up into 3 main steps: Unlocking the Bootloader, Installing a Custom Recovery and finally Rooting. Each new step relies on the previous step to have been completed, and a basic summary of each part is:[2][3]

- **Unlocking Bootloader:** Opens the door to the internal memory of the device to be written on to. This allows you to flash images onto the main partitions of the phone.

- **Installing a Custom Recovery:** A custom recovery is flashed onto the recovery partition of the device and overwrites the stock recovery that exists by default. Custom recoveries bring lots of functionality and give you the ability to perform wipes, install flashable zips, create full backups of your NAND (Nandroid backup), and various other features. An unlocked bootloader is needed to install a custom recovery.
- **Rooting:** You can gain root by either flashing via recovery a pre-rooted custom rom, or flashing a zip containing the SuperSU binaries. A custom recovery is necessary to do this.

After completing these steps your phone will be rooted, the phone will have a custom recovery installed, and the phones bootloader will be unlocked.

Setup, Preparation and Prerequisites

1. Open command prompt - Press Window Key + R, type in "cmd" (without the quotes), and hit enter.
2. Enter fastboot mode- Turn the phone off. Hold volume up + power until the "fastboot" screen appears.

ADB and Fastboot Installation

1. Download the full Android SDK.

2. Extract the zip and place the android-sdk-windows folder on your desktop.

3. Go into the android-sdk-windows folder and run SDK Manager.exe. Install the following packages (there are a total of 4 packages):
- Tools > Android SDK Tools, Android SDK Platform-tools
- Extras > Android Support Library, Google USB Driver.

4. Go back into the android-sdk-windows directory, and you should see a new folder named platform-tools. If you don't see this new folder, repeat the step above.

5. To confirm that it is indeed working, open a command prompt window and enter the following commands:

```
cd Desktop/android-sdk-windows/platform-tools
adb version
```

If it displays "Android Debug Bridge version x.x.xx" it is working. If it is gives an error saying that adb is not a recognized command, it has not been successful. Carefully repeat the steps above if this is the case. Close the command prompt window when you are done.

- **Show File Extensions** - Open a command prompt window and run "Control folders" (without the quotes). Go to the View tab and uncheck the "Hide extensions for known file types" option. This will help avoid confusion when renaming files.
- **Battery** - Ensure that your phone has at least 60% battery remaining, and that your PC is plugged in and won’t shut down spontaneously during the process. The procedure doesn't take very long (5-15 minutes), but it’s best to have enough charge in case something goes wrong.
- **Backup (Optional)** - Unlocking the bootloader will completely wipe all data from the device. This includes apps, settings and even the contents of the internal sdcard (pictures, music, etc.). Copy all important files off the phone onto a PC or upload them to a cloud.
- **Driver Installation** - Download and install the Universal ADB Driver.

Downloads

Download a custom recovery and the SuperSU zip below. Place both files (recovery image and root zip) in the platform-tools folder located on your desktop within the android-sdk-windows folder.

Custom Recovery:

TeamWin Recovery Project (TWRP)

Root:

SuperSU

Unlocking Bootloader

- Turn the phone off. Then boot it into fastboot mode by holding volume up + power. The phone will display "fastboot" text indicating that it has successfully entered fastboot mode.Plug the phone into your PC, then open a command prompt window and type:

  ```
  cd Desktop/android-sdk-windows/platform-tools
  ```

  Code:

  ```
  fastboot devices
  ```

  This command will list the connected devices. If your phones serial number shows up you are good to go and may continue. If the phone is NOT listed this indicates that your drivers are not installed correctly. In order for you to continue you must fix your drivers so that your phone is listed under fastboot devices.

- If the phone has been recognized by the command above, proceed to unlocking the bootloader with the following command: Remember that this step will wipe EVERYTHING off the phone

  Code:

  ```
  fastboot oem unlock
  ```

- After the above command has finished executing, run the following

  Code:

  ```
  fastboot reboot
  ```

  The phone will reboot. Wait until the phone has fully booted up into android, then adjust the following settings on the phone:

- **USB Debugging -** On your phone go to Settings > About phone > Tap on Build number 7 times. This will enable Developer options. Now go back to Settings > Developer options > Enable USB debugging
- **Disable CM Recovery Protection -** On your phone go to Settings > Developer options. Then disable the 'Update recovery with system updates' option.
- Close the command prompt window and proceed onto the next section of the guide.

Installing a Custom Recovery

- Turn the phone off. Then boot it into fastboot mode by holding volume up + power.
- Rename the recovery file that you downloaded above to recovery.img. *Make sure that you rename it to recovery.img NOT recovery.img.img* Remember that this file should be placed in the platform-tools folder inside of the android-sdk-windows folder on your desktop.
- Open a new command prompt and run the following commands:

  Code:

  ```
  cd Desktop/android-sdk-windows/platform-tools
  ```

  Code:

  ```
  fastboot flash recovery recovery.img
  ```

- Once the flash has completed type the following command to reboot the phone:

  Code:

  ```
  fastboot reboot
  ```

After the phone has booted back up, turn it off. Now to enter your newly installed custom recovery, hold volume down + power. The phone should boot into recovery mode. Now that you have a custom recovery, you may continue to the final step.

- Close the command prompt window.

Rooting

Now that your phone has an unlocked bootloader and a custom recovery installed you have a two options to gain root (Pick one or the other. You don't need to do both)

Option A) Flash SuperSU binaries which will give you root with the stock ROM

- Confirm that you have downloaded the SuperSU zip from the downloads section above and that it is located in the platform-tools folder inside of the android-sdk-windows folder on your desktop.
- Turn the phone off then boot into recovery mode by holding volume down + power. Leave the phone at the main screen of the custom recovery for now.
- Open a command prompt window and run the following commands:

Code:

```
cd Desktop/android-sdk-windows/platform-tools
```

Code:

```
adb push UPDATE-SuperSU-vX.XX.zip /sdcard/
```

This will copy the SuperSU zip onto your phone. Once the command has completed continue.

Instructions for TeamWin Recovery Project (TWRP):

- Install > browse to SuperSU zip and select the it
- Swipe to confirm the installation. Then reboot.

Instructions for ClockworkMod (CWM):[6]

- Install zip from sdcard > choose zip from sdcard.
- Next, browse to the location where you previously copied the SuperSU zip and select it.
- To confirm the installation, scroll down to "Yes" and select it. The installation shouldn't take very long, and once it has completed you may reboot.

Option B) Flash a custom Rom which will come pre-rooted

- Note that not all custom roms will be pre rooted, however the majority of them are. Read the OP of the ROM thread to see what the verdict is.
- Copy a custom rom (you can find these in the ONE Android Development and ONE Original Android Development section) onto the phone (remember the location of where you copy it to)
- Turn the phone off then boot into recovery mode by holding volume down + power. To install a custom ROM the general procedure to follow is: factory reset, wipe cache + dalvik cache, flash ROM, flash GApps. Here are the recovery specific instructions:

Instructions for TeamWin Recovery Project (TWRP):

- Wipe > Swipe to Factory Reset
- Install > browse to the location where you previously copied the ROM zip and select it > Swipe to confirm the installation
- Install GApps using same process as ROM, then reboot.

Instructions for ClockworkMod (CWM):[6]

- Wipe data/factory reset
- Wipe cache partition
- advanced > wipe dalvik cache
- Install zip from sdcard > choose zip from sdcard > navigate to the location of the ROM > select the ROM > confirm the installation by selecting "Yes"
- After that you may install the GApps using the same method for flashing the ROM, and finally reboot the phone.

Keep in mind that the first boot after installing a custom ROM & wiping the phone may take longer than usual, as the phone will need to rebuild the dalvik cache and initialize other first boot stuff.

- Open play store and install root Checker app to verify rooting process.[4]

Benefits of rooting and installing custom ROM on device

- The first benefit of accessing administrator privileges over Android is full control over the applications installed on your handset. You can instantly cut the bloat ware and keep only the apps that you really want.

- Rooting Android provides improved backup and restore options.
- You can install different versions of Android.
- You can over clock and under clock the processor.
- Rooting provide you wider range of customization and theming options.
- Rooting provides better speed and battery life.

Threats of rooting and installing custom ROM on device

- You won't be able to use any Internet banking apps. Since after rooting, you will use make rooted apps and they may not provide you safe security.
- There are chances of device getting into boot loop, that means if device is not get rooted properly, it will go into infinite reboot mode.
- Once you root your phone, the manufacturer’s warranty becomes void.
- When you root your phone, you can also flash the device’s ROM using custom programs. Rooting your device will evade lots of these OS-level security features. You’ll be instantly more vulnerable to worms, viruses, spyware, and Trojans. These can be delivered in the form of drive-by downloads, malicious links, and infected apps. One slip and you’ll be exposed; the device won’t be there to bail you out.
- While flashing some ROMs, recovery or even while rooting there is chance that you phone can get bricked and flashing will damage the device kernel.

Conclusion

Rooting provides you freedom of customization even an unlockable bootloader may even be the only way to run and updated version of android on the devices that have stooped receiving updates from the device manufacturer. This is the reason why most of companies provide user a way to unlock the bootloader and install custom builds,. Rooting your Android Phone can be very powerful as it gives you the best of user friendly experience and total control on your device. Remember to always be careful when rooting and custom ROM on your device. However, the step of rooting and custom ROM on your Android Phone should be carefully done. In future work, we have to understand the user’s risk perception of rooting, there should be user awareness and improved root management functionalities. The root apps must provide reliable detection. Our study results suggest that, ultimately, a reliable rooting detection method should be provided by Android OS, with rooting detection logic implemented in the trusted parts of the system, such as integrity-protected kernels or external trusted execution environments.

References

1. https://en.wikipedia.org/wiki/Android_(operating_system)
2. https://forum.xda-developers.com/showthread.php?t=2788632
3. https://forums.oneplus.com/threads/oneplus-one-how-to-unlock-bootloader-install-custom-recovery-and-root.64487/
4. https://android.stackexchange.com/questions/18601/what-exactly-is-superuser-apk-and-su
5. https://rootchecker.com/
6. ClockworkMod Recovery. https://twrp.me/
7. CyanogenMod. http://www.cyanogenmod.org/.
8. https://www.xda-developers.com/
9. https://www.androidauthority.com/benefits-of-rooting-android-284374/
10. https://www.makeuseof.com/tag/security-reasons-never-root-android/
11. https://www.irjet.net/archives/V4/i4/IRJET-V4I4156.pdf/
12. https://www.ijsr.net/archive/v6i4/ART20172750.pdf/